Identity Finder

User Guide

This document is intended to assist with the installation and use of Identity Finder at Montana State University. If you have questions not answered by this document please either visit http://www.identityfinder.com or e-mail identityfinder@montana.edu.

Table of Contents

Background

Identity Finder is the Data Loss Prevention product that was purchased by Montana State University to aid in the identification and remediation of unsecured sensitive data on desktop and laptop computers and servers. The implementation involves a client installed on each computer that will automatically run monthly scans and retrieve any potentially sensitive data for the user to delegate to secure locations. Identity Finder assists in the legal and ethical protection of sensitive data of students, faculty, and staff at MSU.

Identity Finder User Guide and Identity Finder FAQ are available as informational resources. For further assistance, please contact identityfinder@montana.edu.

Installation

1. Navigate to http://www.montana.edu/itcenter/identityfinder/downloads
2. Follow instructions to download the appropriate file for the user's department.

Creating a Profile Password

What is a profile password?

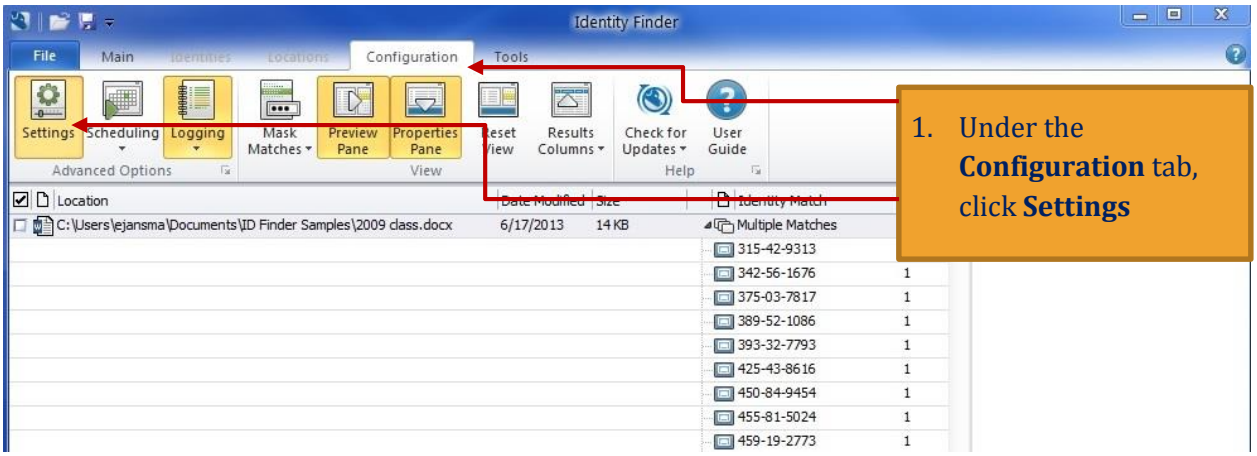
A profile password is required to access saved results and to save settings, new results, reports or locations.

The first time a user opens Identity Finder, a pop-up window will appear and give the option to create a profile password. It is highly recommended users create a password.

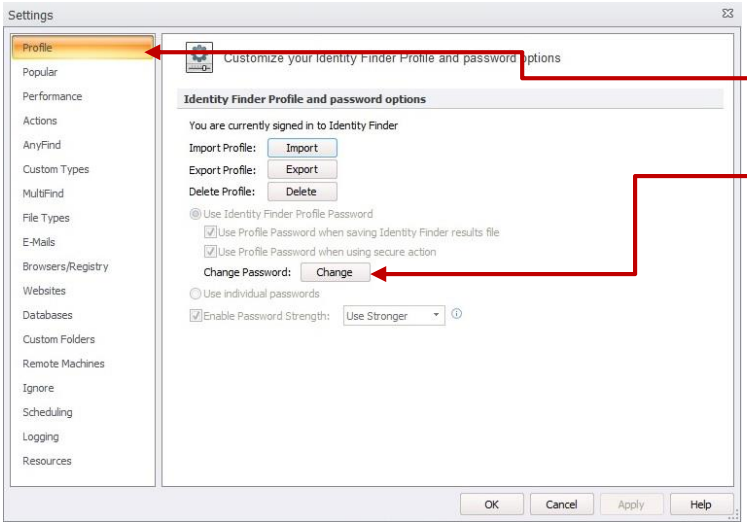
What if I forget my profile password?

Passwords can be reset, however any results saved under a previous password will no longer be accessible to the individual user without the original profile password. Results will still be stored in a central server and remain available to the designated Identity Finder admins.

What if I choose to change my password or set it after the initial install?



1. Under the **Configuration** tab, click **Settings**

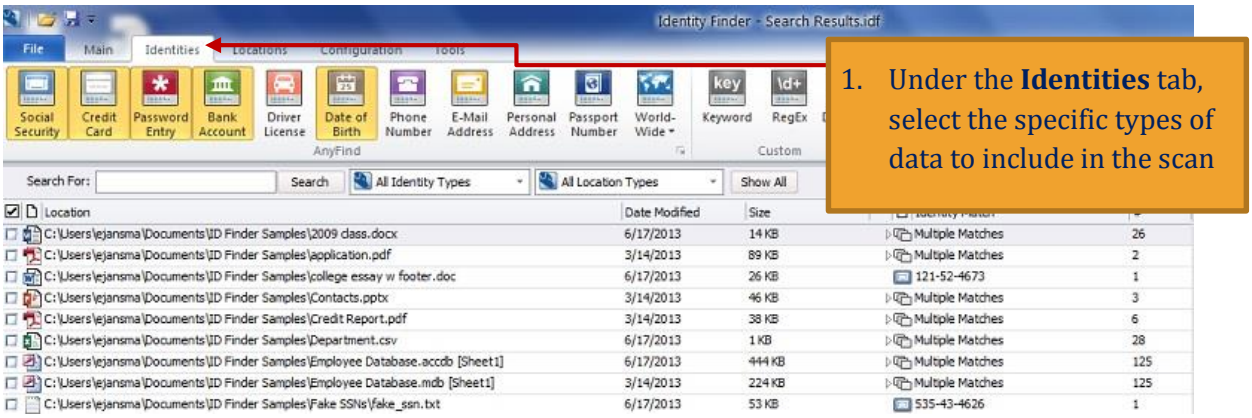


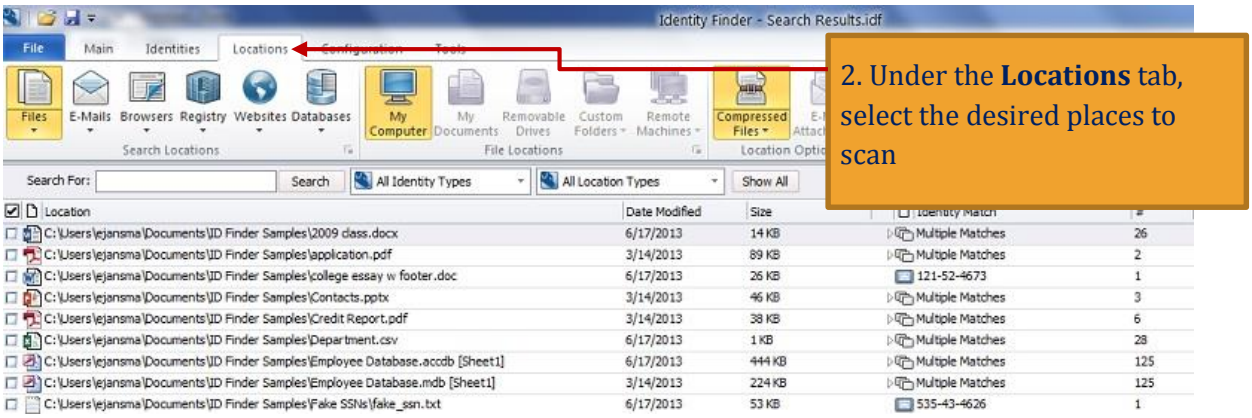
2. Click **Profile** in left column, then click **Change**

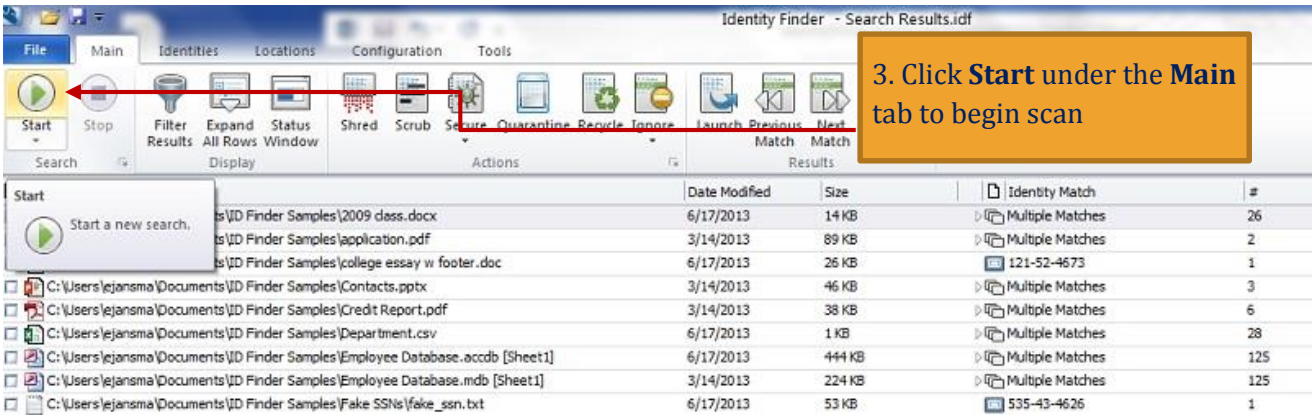
3. Set password/change current password, click **OK**

Scanning a Computer

Identity Finder is pre-set to automatically scan computers for unsecured potentially sensitive data each month. The user may manually initiate a scan separate from the automated scan for specific information at any time.

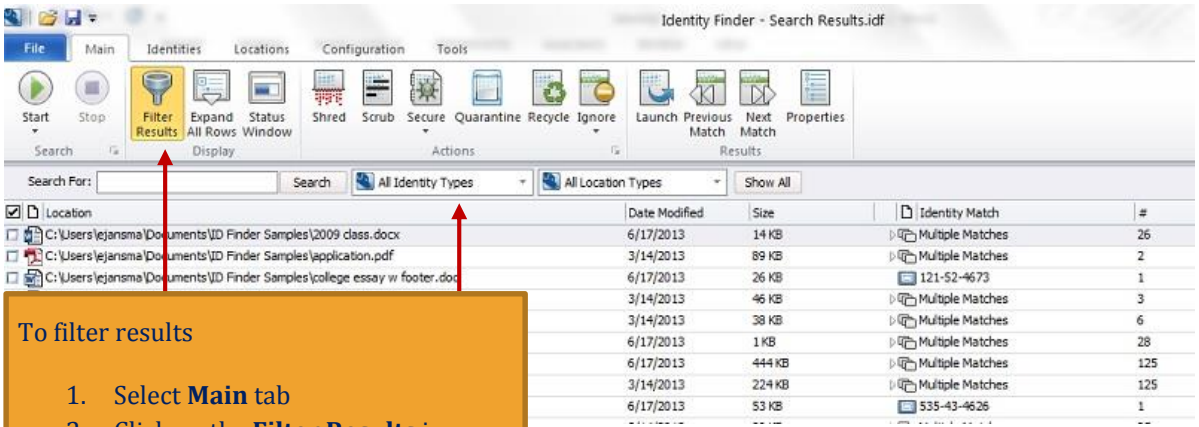






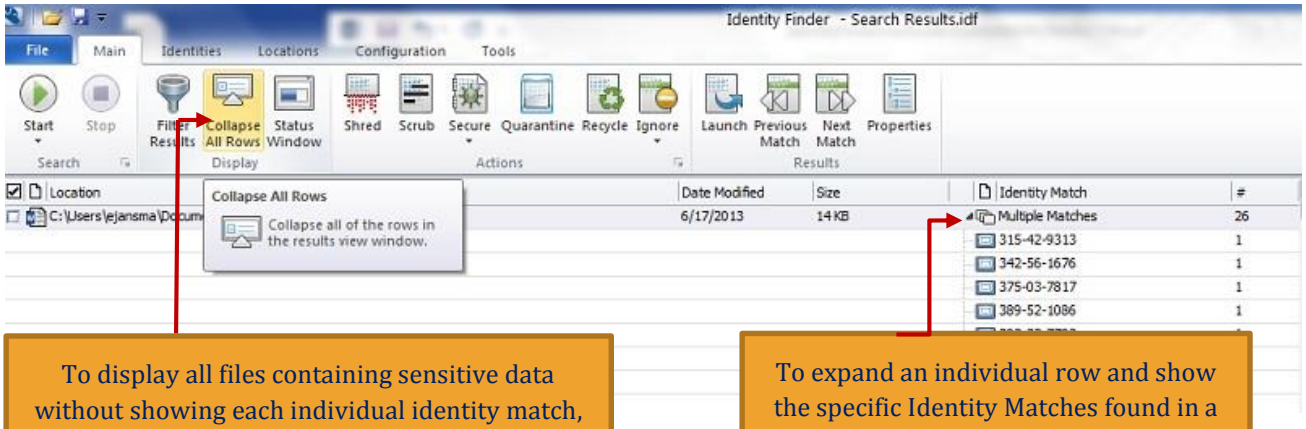
Viewing Results

After a scan is complete, Identity Finder shows the data found by file name and location, what the identity match is, and how many matches within the file were found.



To filter results

1. Select **Main** tab
2. Click on the **Filter Results** icon
3. Use the text box and/or drop down menus to filter according to file name, Identity Types or Locations Types



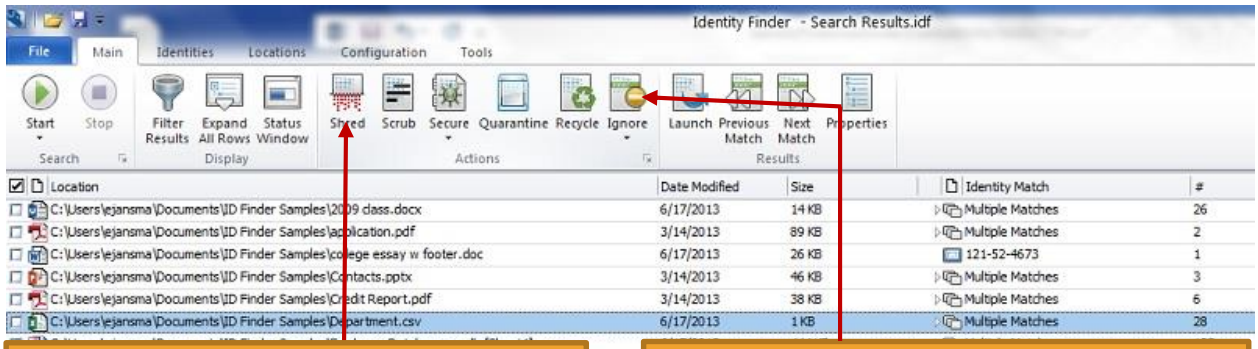
To display all files containing sensitive data without showing each individual identity match, click the **Collapse All Rows** icon under the **Main** tab.

To expand an individual row and show the specific Identity Matches found in a file, click the **black arrow** in the corner of the cell.

Protecting Discovered Sensitive Data

Once sensitive data has been retrieved, users can choose to move the data to the secure network, Knox, delete the data, or keep the data stored as it is.

To secure data, move the files to Knox. If a folder is not already in place for users to secure sensitive data or for questions on how to move files from an unsecure location to Knox, visit http://www.montana.edu/knox



To delete a file(s)

1. Click the box next to the file location to select it
2. Under the **Main** tab, click the **Shred** icon to permanently delete the file

To ignore a file(s)

1. Click the box next to the file location to select it
2. Click the **Ignore** icon to keep the file in its current location and exempt it from future scans