Identity Finder

Identity Finder is a tool designed to help you search your computer for data that may contain Level 4 confidential information such as credit card numbers, or social security numbers. It can also securely delete such information for you. Identity Finder works by searching your computer for files containing specific patterns of numbers and letters.

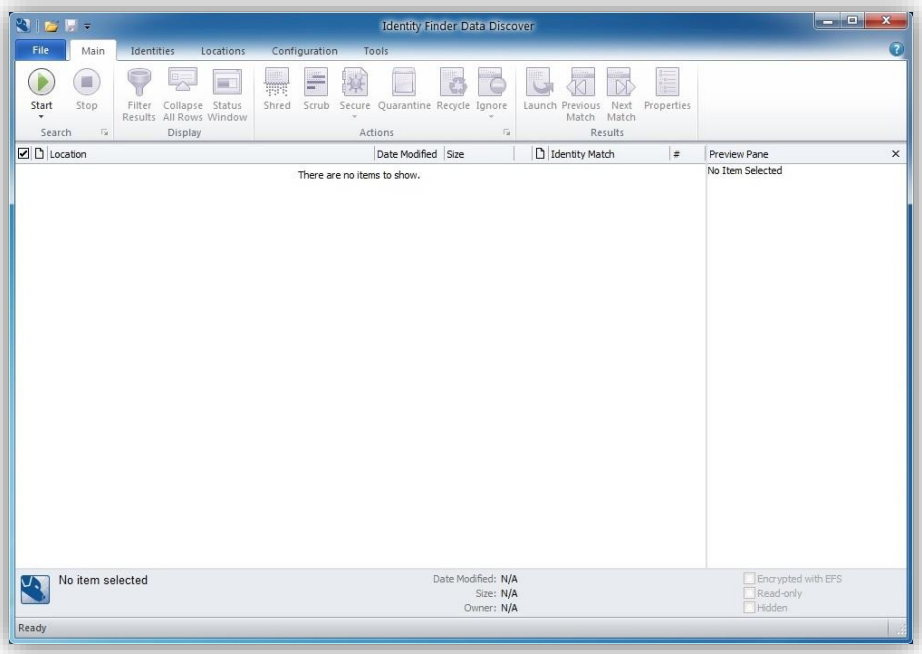
How to scan your computer for sensitive information

To scan your computer manually for sensitive information:

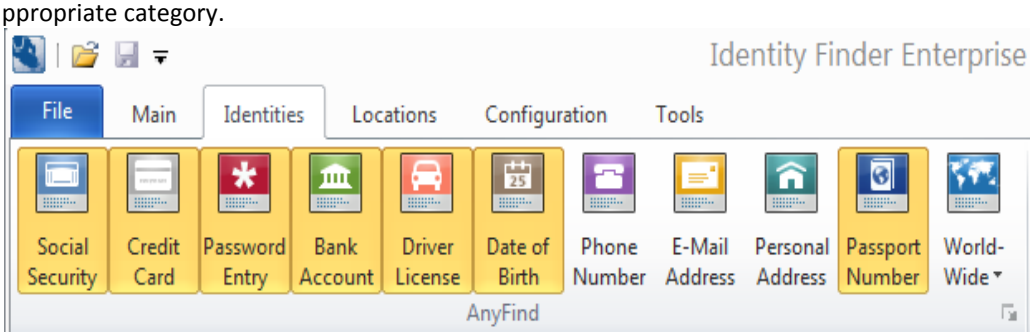
1. Close any web browser window.
2. Run the Identity Finder program: **Start Menu → Programs → Identity Finder → Identity Finder**.
3. If this is your first time using Identity Finder, you will be asked to create a **New Identity Finder Profile**, and be prompted to enter and confirm a password. It is advised that you create a unique password solely for Identity Finder.

4. After entering your password, your Identity Finder Profile password will be set. Click **OK** to dismiss this message and continue.

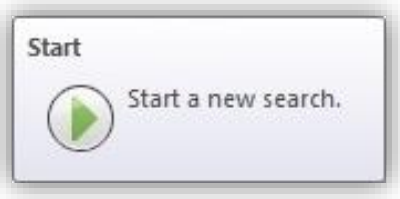
5. You will now be at the **Identity Finder Data Discover Window**.



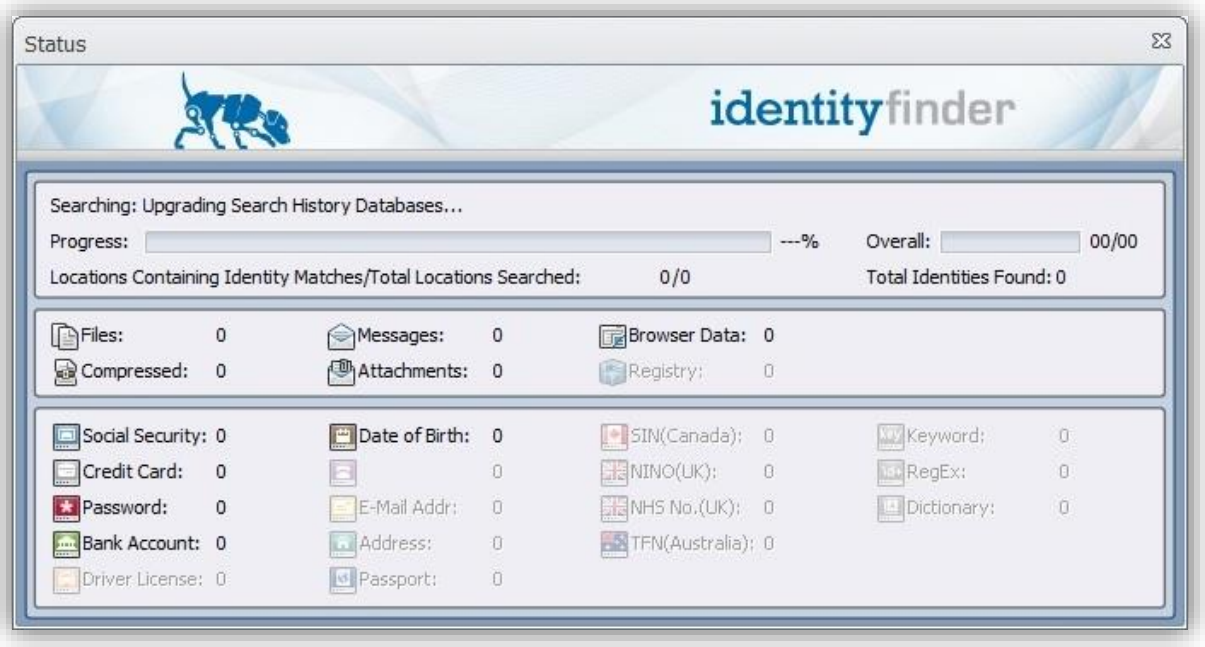
6. Prior to initiating a scan, you can click on the **Identities Tab** to change the selected search criteria for Identity Finder**.** HUIT recommends you search for Social Security Numbers, Credit Card Numbers, Password Entries, Bank Account Numbers, Driver License, Date of Birth, and Passport Numbers. You can expand your search to include other classes of HRCI by selecting the appropriate category.



7. In the **Main** tab, click **Start** to initiate a scan.



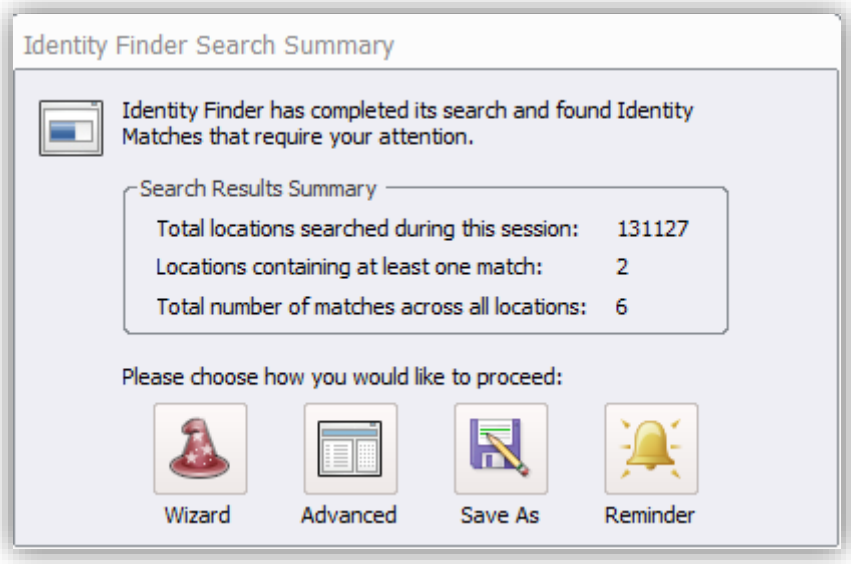
8. A **Status** window will now be visible. Identity finder will be searching for the highlighted materials across your computer. You can continue to work while Identity Finder scans your computer. **However, using Internet Explorer or Firefox will interfere with Identity Finder's ability to search browser data stored on your computer.**



9. If Identity Finder found sensitive data, you will be given options via the **Results Wizard**. The remediation window is divided into several sections: **Actions**, **File Browser** and the **Preview Pane**. Selected items in the File Browser will display in the Preview Pane, with any suspected HRCI highlighted in yellow. Review the information for accuracy prior to taking action.

   ***Important*: Some results in the File Browser may be false positives, including system files and program files that your computer needs in order to run properly. These may include files that end in .exe, .ini, .dat, and .dll. Deleting program or system files may cause programs not to work correctly, and can even make your computer inoperable.**

10. Once your scan is completed, a window will pop up with a summary of your results.

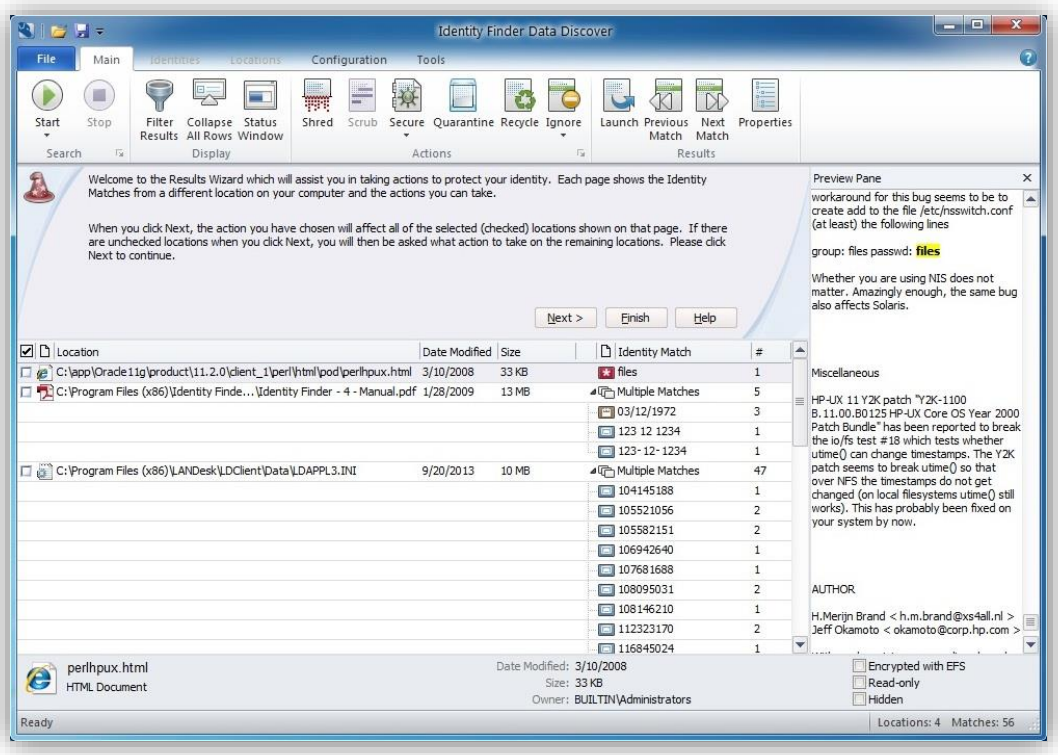


- Wizard: The **Results Wizard** is an easy to use, quick way to secure your results using Identity Finder. By default you will be prompted to use the **Results Wizard** when Identity Finder is finished searching your computer. However, you can also initiate the wizard by clicking **Main** ribbon, then the **Start Results Wizard** dropdown on the **Start** button any time after your search is complete while there are still results in the Results View.
- The Advanced Options setting provides you access to advanced features within Identity Finder that are recommended for power users only.

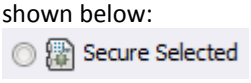
- Save As: Identity Finder allows you to save the results of your searches in three ways:
    - **Identity Finder**: Generates a *.idf file, which is encrypted with a password of your choice and cannot be read by anyone else. Files saved in this format can only be opened from within Identity Finder and allow you to work with your results at any time in the future. This format is useful when you have run a search but wish to take action on your results at a later time. All results are saved and secured using this format.
    - **Web Page Report**: Generates a report as a *.html file, which contains an analysis of your results including summary information and totals for the number and types of identity matches that were found as well as the locations containing those matches. This report can be used to show trends if you compare it to previous reports. The Web Page Report is not secured and potentially contains location and identity information so you must be careful to protect it. After you are finished with a file in this format, you should use the Identity Finder tools to shred it.
    - **Text Export**: Generates a Comma Separated Values (*.csv) file, which is saved unencrypted, in clear text and can be read by anyone with access to your computer. Files saved in this format can be opened in any text editor or spreadsheet program such as Microsoft Excel but cannot be loaded back into Identity Finder. This format is useful when you wish to perform advanced searching, sorting, and reporting of your data in another application. After you are finished with a file in this format, you should use the Identity Finder tools to shred it.

- Reminder: If you choose to be reminded later, you are presented with several time options. Identity Finder will minimize itself to your system tray and remain there until the specified period of time has passed. If you want to bring Identity Finder back sooner, you can double click the System Tray icon.

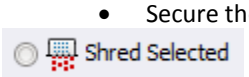
11. Select the “Wizard” option and click “Next”.



12. Once you finish reviewing the file, you must take an appropriate action. A listing and description of all available actions is shown below:



- Secure the highlighted item using the associated application’s features.



- Shred implements the U.S. Department of Defense deletion standard, which is known as DOD 5220.00-M for deleting files.

Recycle Selected

- Delete the highlighted file by moving it to the 'Recycle Bin'. Note: This does not actually delete your file and has a high probability of being recovered even after you empty the Recycle Bin. It is recommended you use the "Shred" button instead.

Quarantine Selected

- Move the highlighted file to a quarantine location and permanently shred it from its original location.

Ignore Selected Locations

- Ignore either the currently highlighted item or its Identity Match so that it is not found again. Note: Item on the Ignore List will not be searched. To remove an item from the Ignore List, use the 'Manage Ignore List' option.

Skip Remaining Items

- These items will be skipped for now, but will return in following scans.

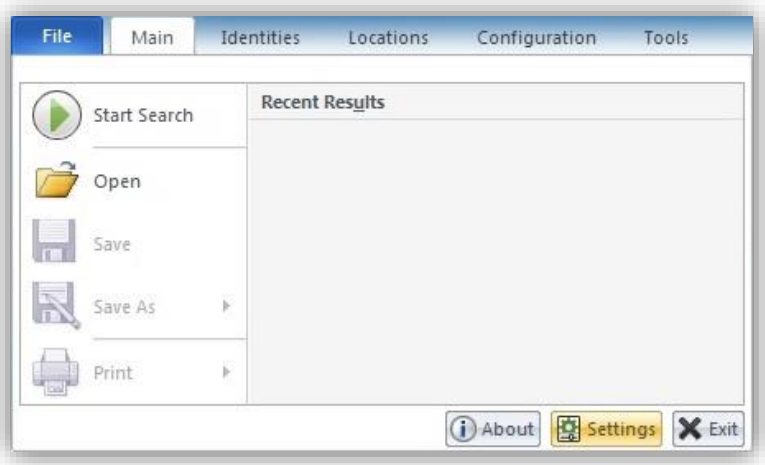
HUIT Security policies dictate that HRCI data is not to be saved locally to any machine. If Identity Finder discovers any HRCI data on your computer, please make sure to move it to an approved location for HRCI data. Once data is moved, you may use the Shred option to remove it completely from your machine. For more information about HRCI information, please see this site: http://security.harvard.edu/files/it-security-new/files/data_classification_table_abridged_7.23.13_0.pdf.

Scheduling a recurring scan

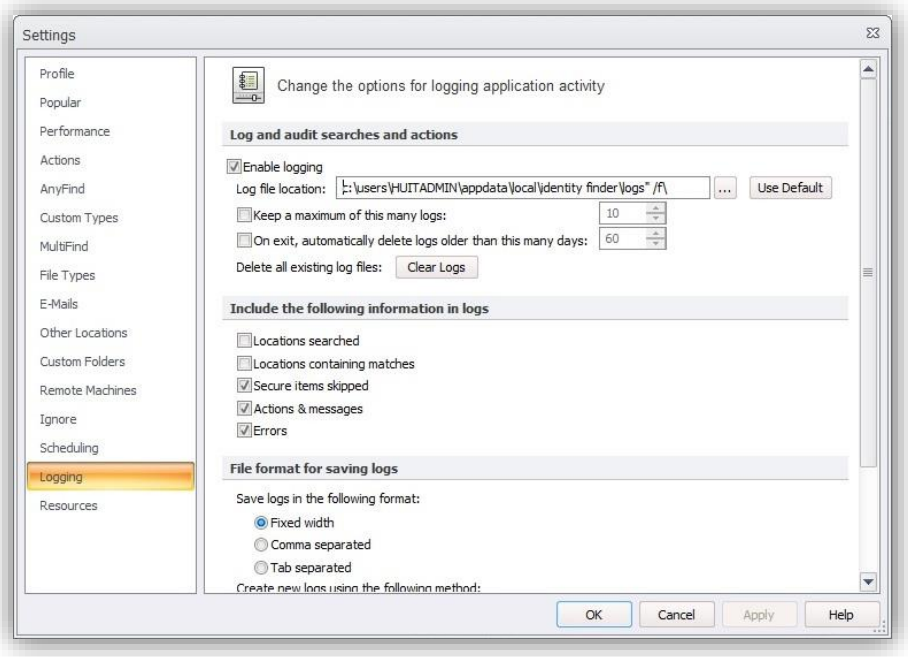
In order to aid you in keeping your computer free of high-risk confidential information, HUIT suggests that you schedule a monthly scan for Identity Finder, but actual recurrence may be based on your department needs. To set up an automated scan, follow the steps below.

***Important*: After your initial scan, subsequent monthly scans will complete faster, searching for any newly added documents that may contain High Risk Confidential Information.**

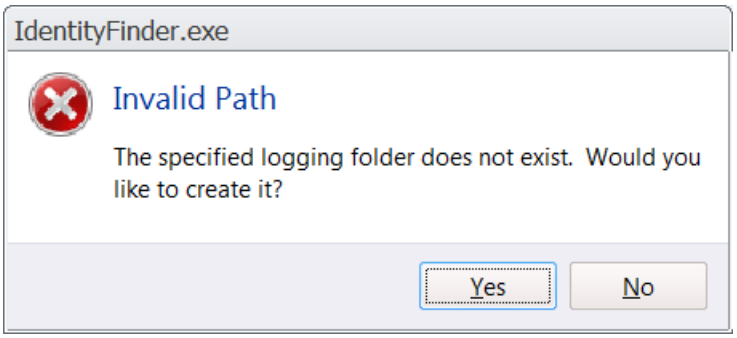
1. Run the Identity Finder program: **Start Menu → Programs → Identity Finder → Identity Finder**.
2. On the top toolbar, click **File → Settings**. A new Settings window will open.



3. In **Settings**, click **Logging** on the left sidebar.
4. In the Logging pane, Click **Enable logging**, and the **Use Default** Button. Click **Apply** at the bottom of the window when done.

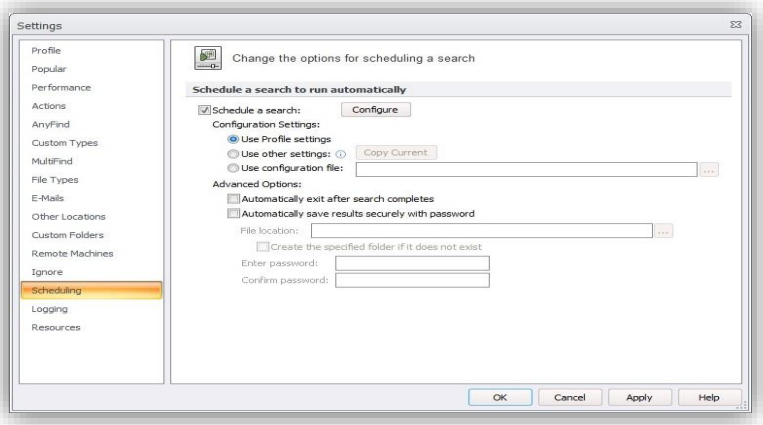


a. Note: If this is the first time you are enabling logging, you will be presented with this window:

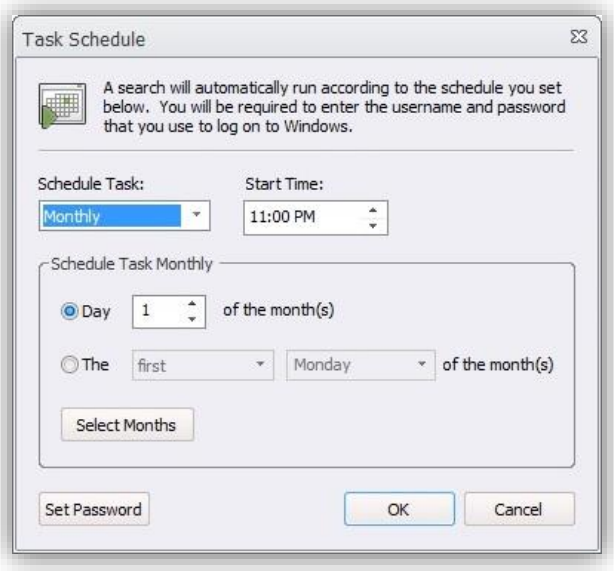


b. Click yes.

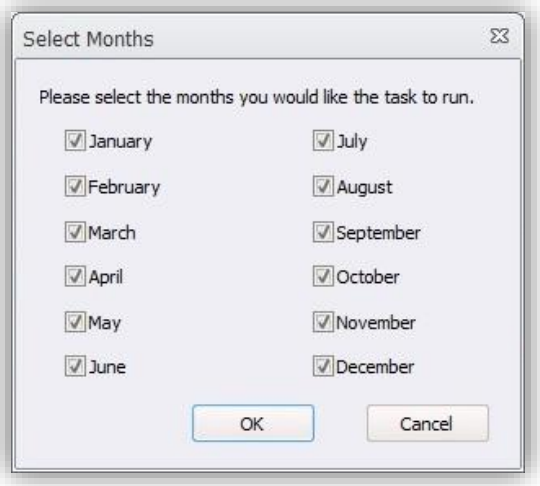
5. After applying the logging settings, click **Scheduling** on the left sidebar.



6. Under **Scheduling a search to run automatically**, check **Schedule a search**. Then click the **Configure** button.
   a. You will see a new window, titled **Task schedule**.



i. Under **Schedule Task**, select the required schedule (in this example, Monthly).
ii. Under **Start Time**, select **10:00 AM** (or a time convenient to you, when your computer is turned on and operational)
iii. Under **Schedule Task Monthly**, select **Day 1 of the month(s)**.
iv. Click the **Select Months** button. A new window titled **Select Months** will appear. Ensure that the required months are checked. (See below.) Click **OK**.



b. Click **OK** to save all settings and close the **Task Schedule** window.

7. Click **Apply**. You will be prompted for a **User Name** and **Password**. Enter the user name and password that you use to log in to your computer. Enter your password in both password fields. Then click **OK**.

a. You should be back at the window titled **Settings**. **Click OK** to exit this window.
b. If you see the following error message, click No.

c. The scheduled scan will now run automatically at the time you selected.