

Identity Finder for Mac

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.

Below are basic instructions on how to scan your computer for sensitive data. You can also access the web-based help at <http://www.identityfinder.com/help/mac>.

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: **Applications** → **Identity Finder.app**.
3. If this is the 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.



The screenshot shows a dialog box titled "Identity Finder Profile Password". It contains a document icon with a gear, the title "New Identity Finder Profile", and explanatory text: "Your Profile allows you to save your settings and automatically use your Profile Password when securing results or saving reports. You will be asked for this password when Identity Finder starts and when opening secure results and reports." Below the text are two input fields: "Enter Password:" and "Confirm Password:". At the bottom right are "Cancel" and "OK" buttons.

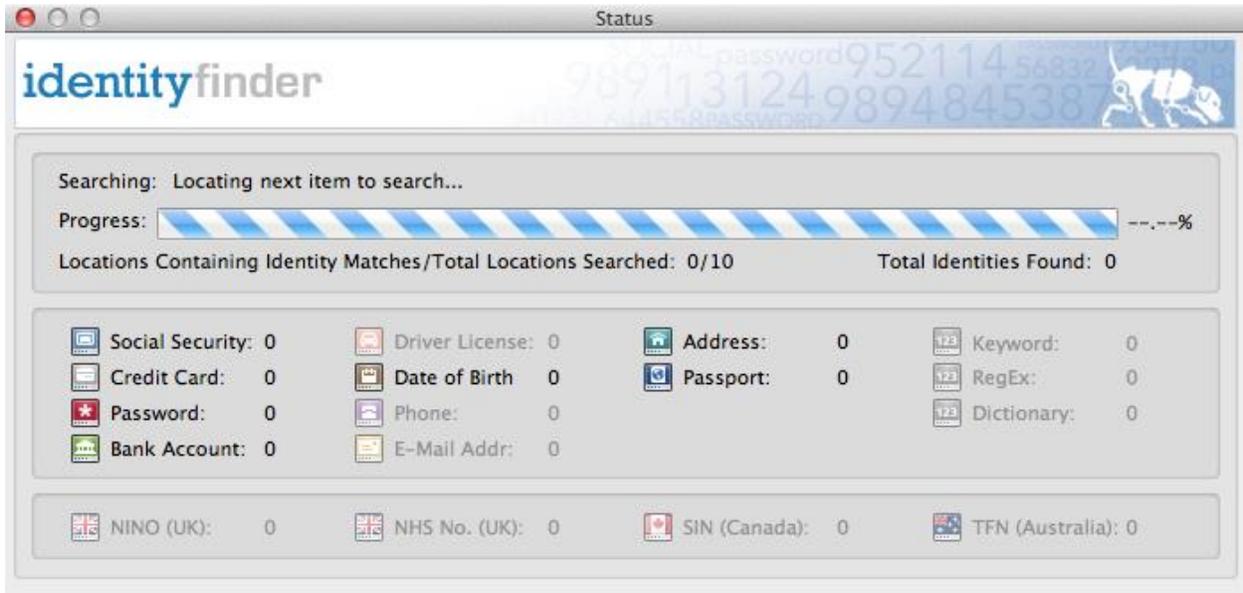
If this is not the first login, you will still need to enter your password at the window below



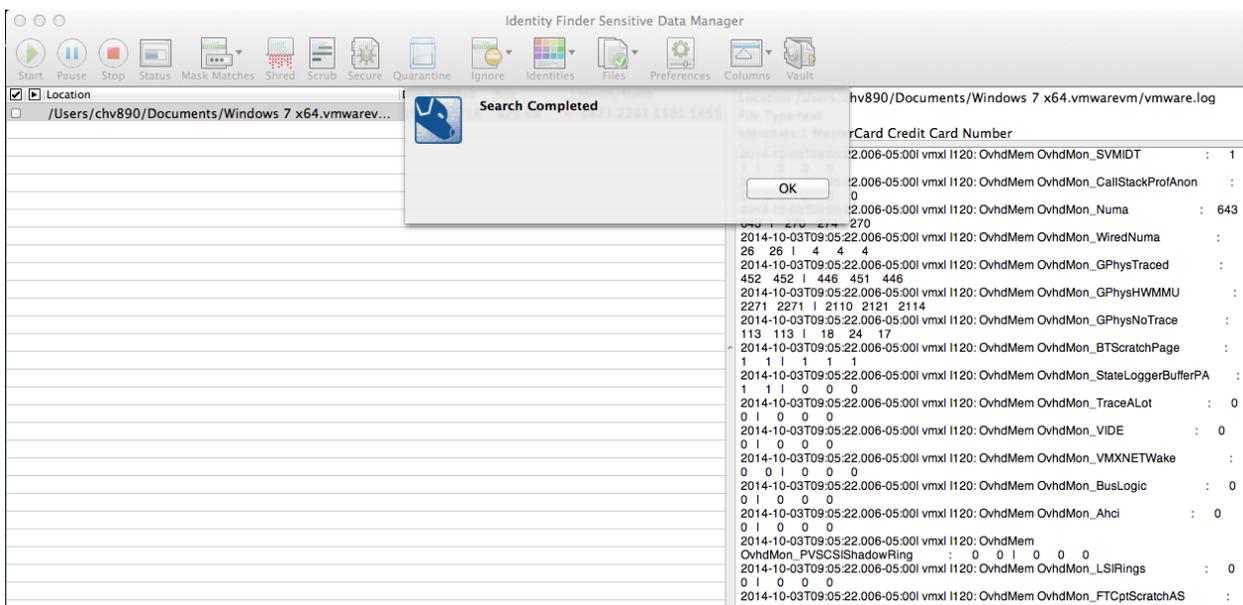
4. You will now be at the **Identity Finder Search Setup Window**. HUIT recommends you search for Social Security Numbers, Credit Card Numbers, Password Entries, Bank Account Numbers, Date of Birth, Personal Addresses, and Passport Numbers. You can expand your search to include other classes of HRCI by checking the appropriate box.



- Click **Search** to initiate a scan.
- 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 a web browser will interfere with Identity Finder's ability to search web data stored on your computer.**

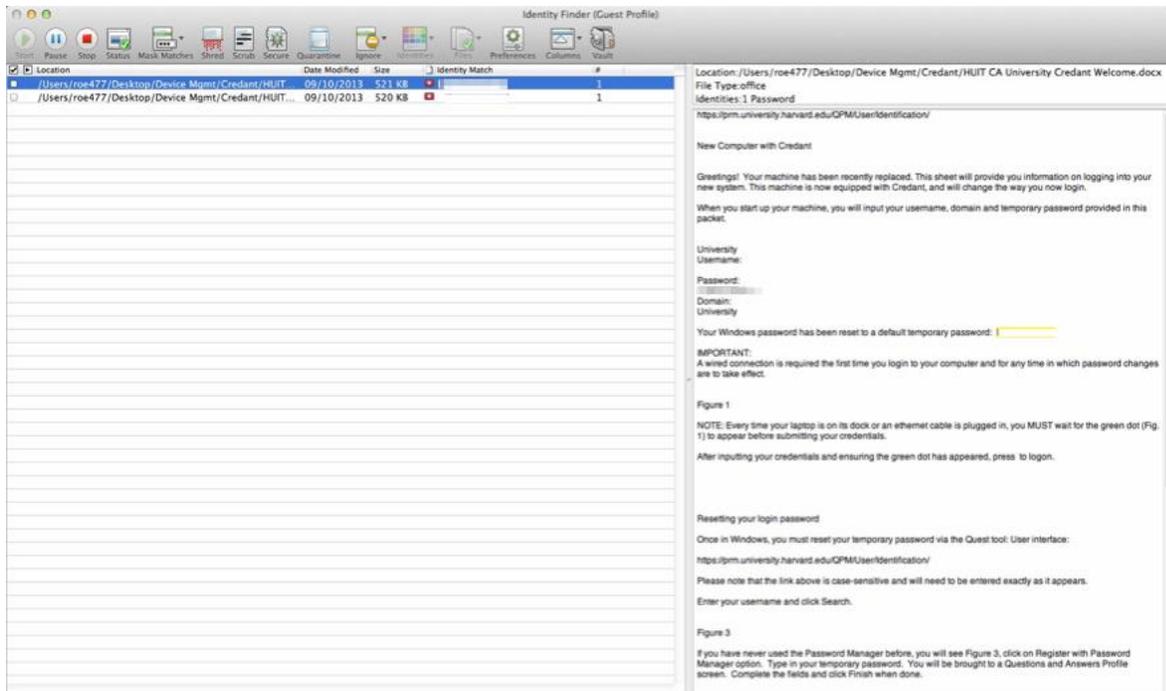


- When the scan is complete you will be directed to the Identity Finder Sensitive Data Manager window with a drop down indicating, "Search Completed." Click "OK".



8. If Identity Finder found sensitive data, you will be given options to remediate the files. The left side of the window will show the name and location of the file and the right will display a preview of the currently selected file, 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 .plist and .dat. Deleting program or system files may cause programs not to work correctly, and can even make your computer inoperable.



9. Once you finish reviewing the file, you must take an appropriate action by selecting the file with the checkbox to the left of the name and then choosing one of the actions on the menu bar. A listing and description of all available actions is shown below:

Shred



Shred implements the U.S. Department of Defense deletion standard, which is known as DOD 5220.22-M, for deleting files.

Scrub



Remove the highlighted information from the location while keeping all other data intact.

Secure



Secure the highlighted item using the associated application's features.

Quarantine



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

Recycle



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.

Ignore



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.

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

If you are unsure about what action to take with respect to any sensitive data found by Identity Finder, please speak with your manager. For any technical concerns, please feel free to contact the HUIT Help Desk at ithelp@harvard.edu or 617 495-7777 for assistance.