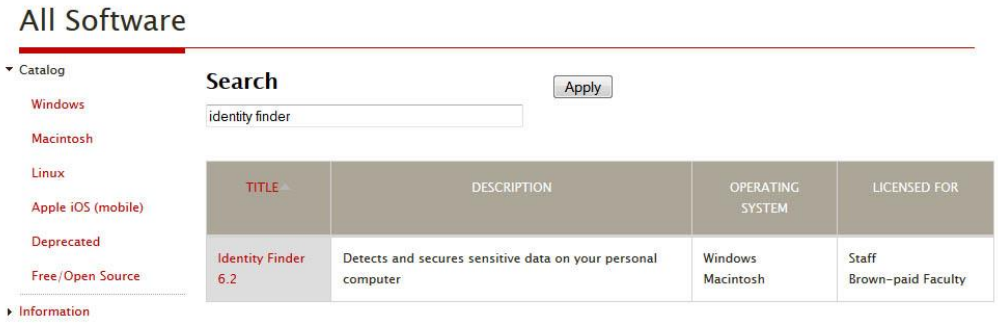
Using Identity Finder

To find and secure personal information on your computer, the Information Security Group recommends that you install and periodically run Identity Finder (IDF), which helps prevent identity theft and aids in keeping Brown compliant with federal and state laws by detecting and securing sensitive data on your computer. IDF is able to detect patterns – such as those for Social Security, credit card and bank account numbers, references to passwords and other customizable data that you would specify.

All active employees – faculty and staff – can download and install the full enterprise version of IDF from the Software download pages onto their Brown computers (runs on both Windows and Macs). In addition, software is available from the Identity Finder website for use by students and home users, including a free application, Password Sweeper.

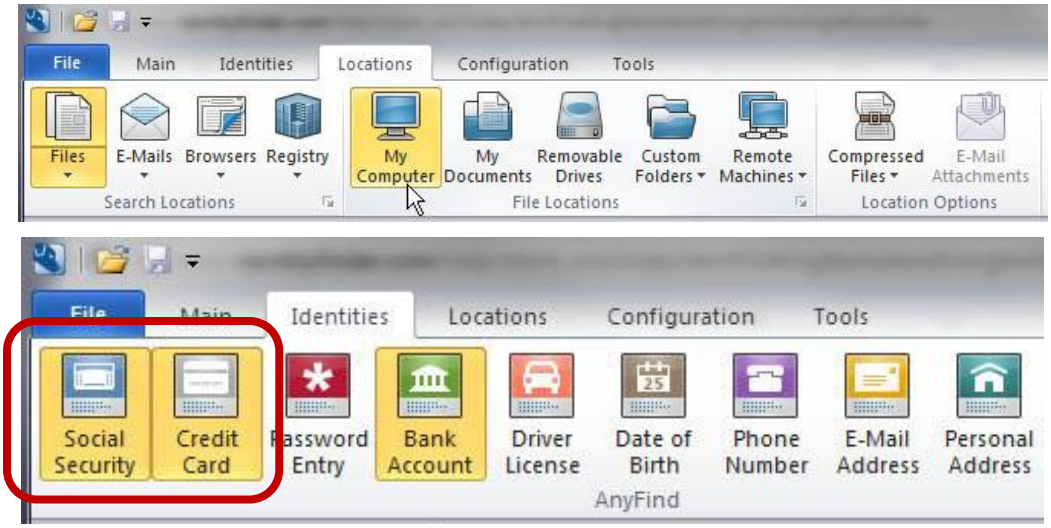
☐ **Install Identity Finder.** Faculty and staff can download IDF from the Software Catalog. A link is also available at **brown.edu/go/identityfinder**. Versions for students and home use – Password Sweeper (free), Identity Sweeper ($29.95) and Identity Sweeper Pro ($39.95) – can be found at identitysweeper.com/products.



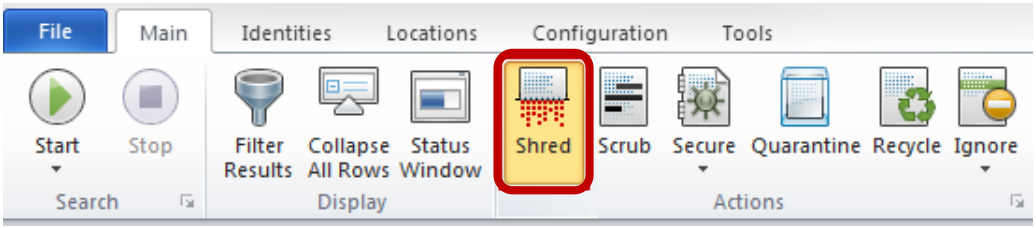
☐ **Follow the Setup Wizard to activate the software** (installation instructions can be found on the download page) then create a password to secure your reports.

☐ **Define your search**: what drive(s), types of files, kinds of PII. To meet regulatory compliance, ISG recommends searches of your hard drive that target social security and credit card numbers. This data is at highest risk and searches for it produce the fewest false positives.

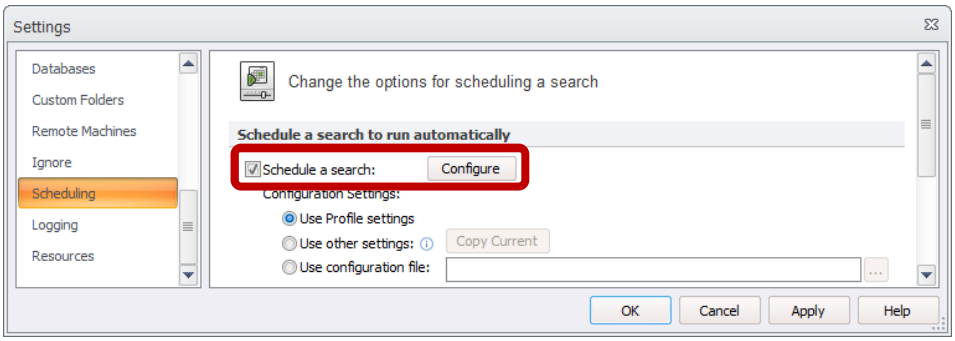
Configure your search to locate credit card numbers and SSNs.

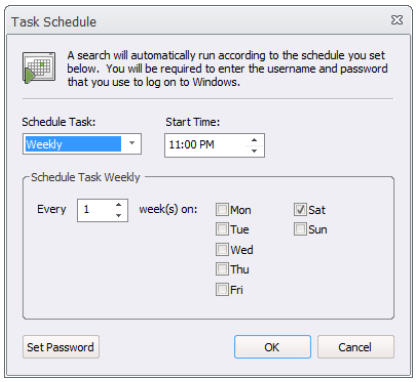


☐ **Protect any discovered PII** by destroying or securing it (Shred, Scrub, Secure and Quarantine).



☐ **Schedule regular runs.** How often depends on what kinds of PII you routinely deal with. If you handle SSNs and bank account information in your daily work, ISG recommends once a week, and if otherwise, quarterly at a minimum. Note that you may wish to broaden your search to other sensitive information, such as passwords, after initial scans for high risk PII.





For questions about using the software, visit **brown.edu/go/identityfinder**, which includes links to the online manuals for both Windows and Macs. The page also includes recommendations on when to use the various protection options with examples of each. For questions about policy and/or procedures, contact ISG@brown.edu.