California State University
SAN MARCOS

Information Security Office
Instructional & Information Technology Services

333 S. Twin Oaks Valley Road San Marcos, CA 92096-0001
securityteam@csusm.edu www.csusm.edu/security

Working With Your Identity Finder Results

You can take the following actions with each result in Identity Finder:

- **Shred:** deletes the file containing protected information from your computer.
- **Secure:** password protects the file. Contact securityhelp@csusm.edu if you have any questions.
- **Ignore:** adds the item to a list of findings to ignore on subsequent searches. **NOTE:** Ignore should only be used for false positives!

False Positives

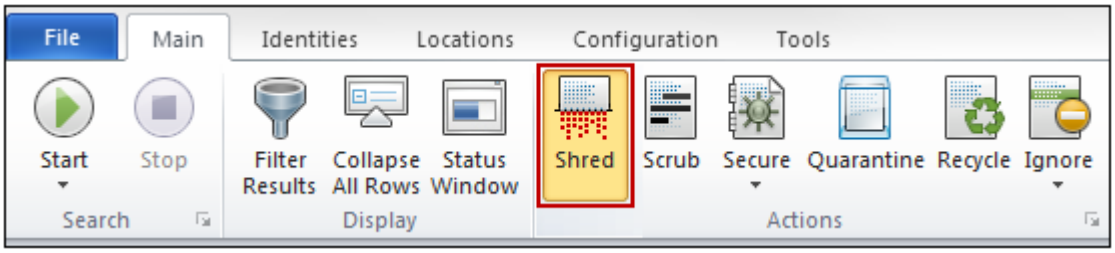
Not every result returned by Identity Finder is going to be protected data. For example, on our campus student ID numbers are 9 digits long and can often be mistaken by Identity Finder as Social Security Numbers. Therefore it is necessary for an individual to review each result of the Identity Finder scan.

Shred

Shredding a file removes it completely from your computer. This cannot be undone, so shred carefully!

Shredding a file containing protected information is the appropriate action to take when you no longer need the file or the protected information it contains.

To **Shred** a file, select the file in the Results Pane and click Shred in the Main ribbon.

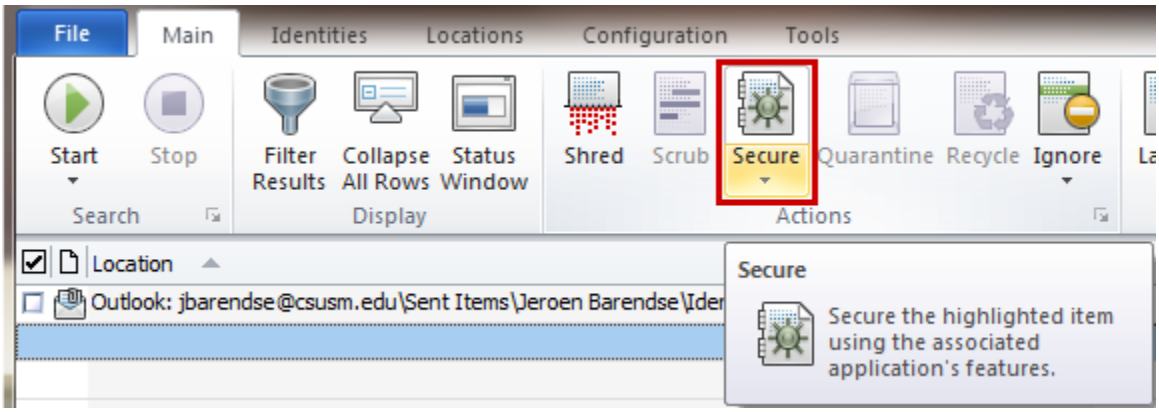


Secure

Secure password protects the file with a password chosen by you.

Secure should only be used as a last resort for files that contain protected information that you have a business need to retain.

To **Secure** a file, select the file in the Results Pane and click Secure in the Main ribbon.

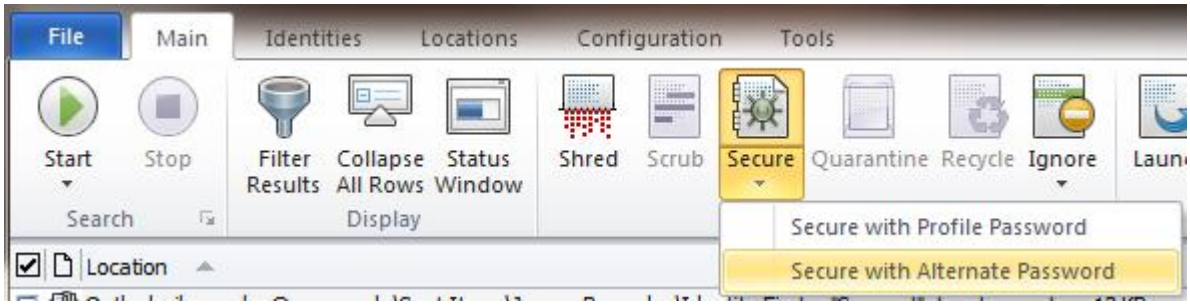


When you click Secure, Identity Finder automatically password protects the selected file with your profile password. When securing files in a Department Share, your files must be secured with an alternate password.

Please create an alternate password and email this password in an encrypted email by typing "csusm-encrypt" (without quotes) in to the subject line and email to the Information Security team at infosec@csusm.edu.

Securing With an Alternate Password

You will be prompted to secure the item with either your profile password (which you entered upon starting Identity Finder) or an alternate password. Select alternate password.



California State University
SAN MARCOS

Information Security Office | 333 S. Twin Oaks Valley Road | San Marcos, CA 92096-0001
Instructional & Information Technology Services | securityteam@csusm.edu | www.csusm.edu/security

<u>WARNING!</u> If the password used to secure a given file is lost, this file cannot be recovered! You may write down any file passwords and the associated file name and deliver this list to the Information Security Team for safe keeping. Again, if a file's password is lost, the file is NOT recoverable.

You may also email password to infosec@csusm.edu in an encrypted email by typing "csusm-encrypt" in the subject line.