Identity Finder Quick Start Guide for Mac

Maintained by University IT Security and Policy
Revised date: 9/17/2015

Identity Finder assists in the discovery and removal of Personally Identifiable Information (PII) from University owned computers. Faculty and staff should run this tool on their computers.

In this document

Your responsibilities

As a faculty or staff member at the University of Rochester, your responsibility is to limit the use of and protect PII. The Identity Finder software is made available to assist in locating and cleaning electronic data stores containing PII.

You are responsible for installing Identity Finder on your computer and running the first scan. You must then review the results and take action on each file. The instructions below outline how to perform these tasks, and the options you have for remediation.

Even if your computer is encrypted with Sophos SafeGuard, FileVault or other encryption software, you are still required to run Identity Finder to identify and clean up PII stores. Encryption only protects against data retrieval if the computer has been stolen – other attacks such as malware or network intrusions still leave data at risk. Data that must be kept should be registered under the Social Security Number Registry, maintained my University IT. Register here: http://tech.rochester.edu/forms/register-restricted-data-collections/

Privacy statement

University IT does not collect the PII match data from Identity Finder. This means the individual SSN, credit card, or other results found by the software are not sent to University IT. The data that is collected by University IT when a scan is run is limited to:

- Location of files and email messages with PII
- Types of PII found (SSN, credit card, bank account, etc)
- Actions taken to clean up the PII collections
- User name that ran Identity Finder
- Computer name and IP address
- Date and time the scan was run

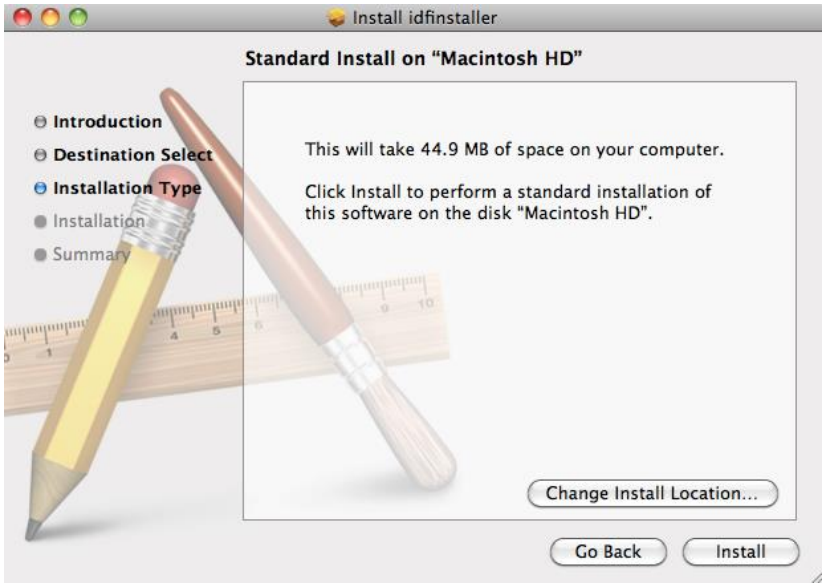
Installation

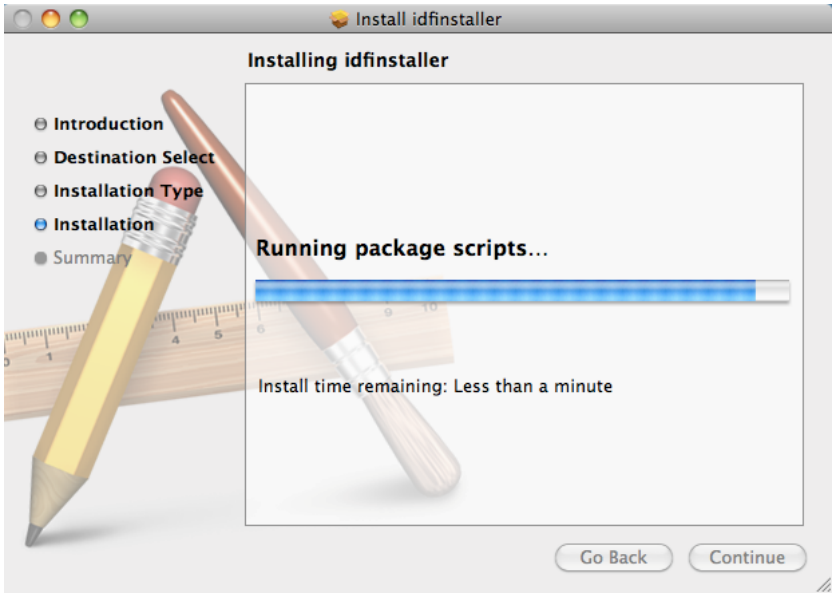
1. Download the installer from the Security and Policy website and save it on your computer.

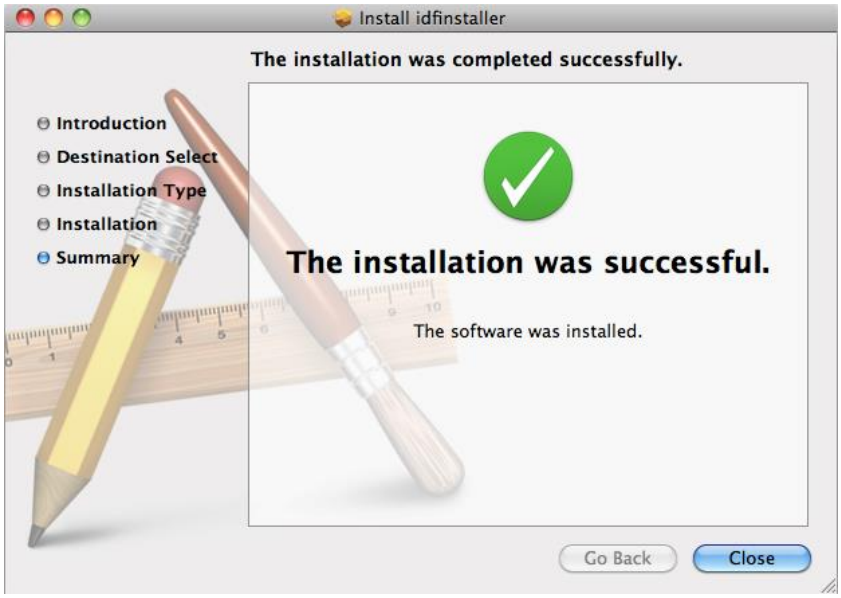
Note: Your computer must be connected to the University of Rochester network for the duration of the installation. The University network includes being physically plugged in on campus, connected over the UR_Internal_Secure, UR_Connected wireless networks, or over VPN. UR_RC_Guest will not work.

2. Run the installer and click Continue:

3. Click Install and allow the installer to complete:





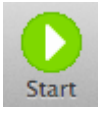


4. When you start Identity Finder, you may be notified that AnyFind Defintions have been updated.

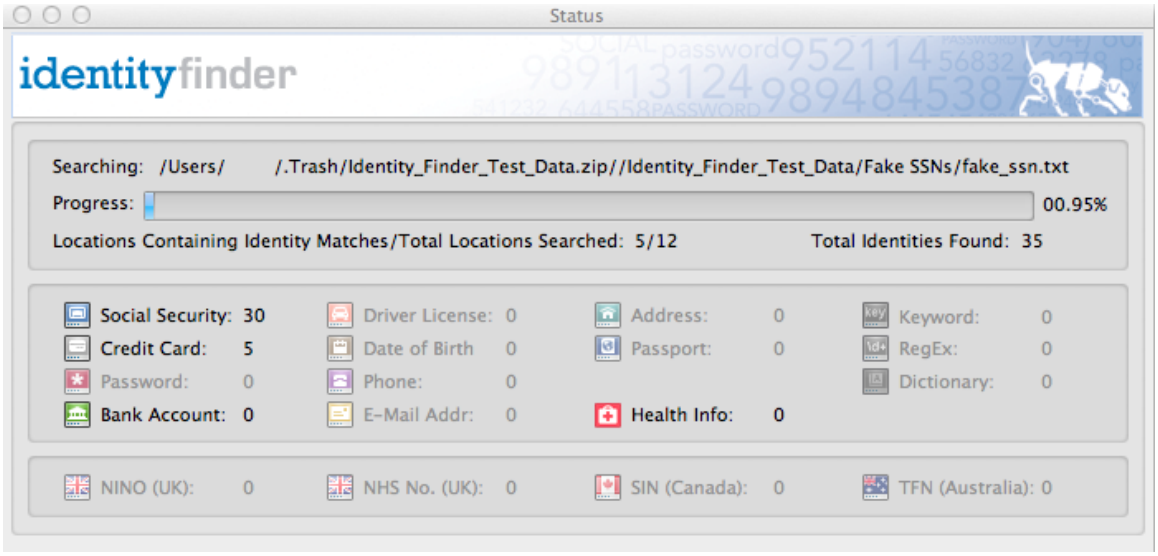
First scan after installation

Launch Identity Finder from the Applications folder on your computer.

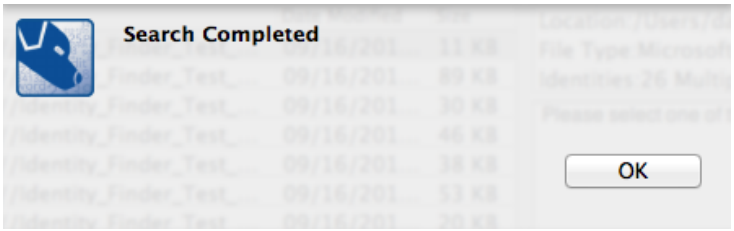
Note: The first scan may take several hours and may slightly impact the performance of your computer, so it is recommended to run it at the end of the day when the computer can be left on overnight. Subsequent scans will be much quicker, as only files that have been created or changed since the last scan will be checked.

Identity Finder is preconfigured by University IT with specific settings. To get started with a scan that looks for Social Security, credit card numbers and bank account numbers in your email and all files on locally connected devices (thumb drives and CD-ROMs included), simply click the 

button in the Identity Finder main window. The search begins.



When the scan is complete you will be notified of the results, and you can take action on what Identity Finder has found.



Remediation

Upon completion of the scan, Identity Finder will present a report of all PII found with options to electronically **Shred** (delete), **Scrub** (redact), or **Ignore** the data. You must review and remediate all results – meaning they must be removed, replaced or moved to a network share.

How do I decide what to do with the results?

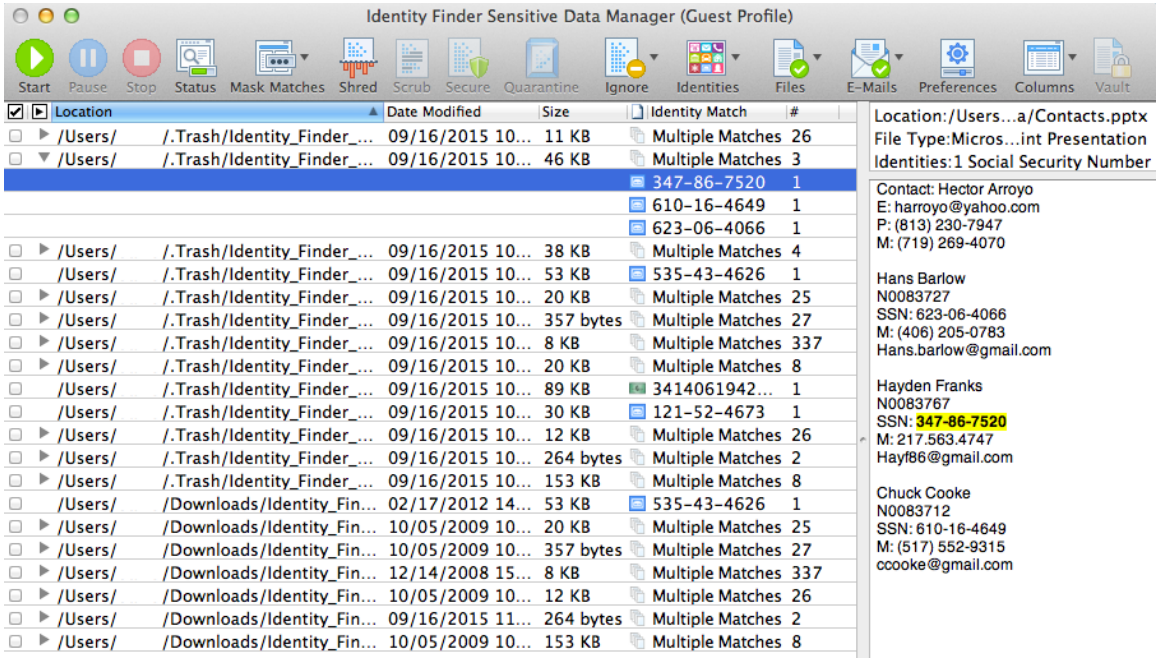
Follow this set of guidelines when determining what action to take on a file or email message with PII:

1. If the **files are no longer needed**, *Shred* (delete) them - even if they are documents that reside in email.
2. If the **files are needed, but the identifying information is not needed**, remove the identifying information from the files. The *Scrub* function in Identity Finder is able to do this with some file types.
3. If the **match is a false positive**, use the *Ignore* option within Identity Finder to remove them from the results list. You only have to ignore a file or match one time – once the collection is ignored, Identity Finder will NOT flag it in successive runs.
4. If the **files are needed and the identifying information must be kept**:
    a. Determine if they can be moved to a more secure location such as a department file share.

b. If the file can't be moved, do not take any action with Identity Finder.
    i. Validate that your PC/Mac is encrypted.
    ii. The collection/machine **must** be reported to University IT through the following website - http://tech.rochester.edu/forms/register-restricted-data-collections/

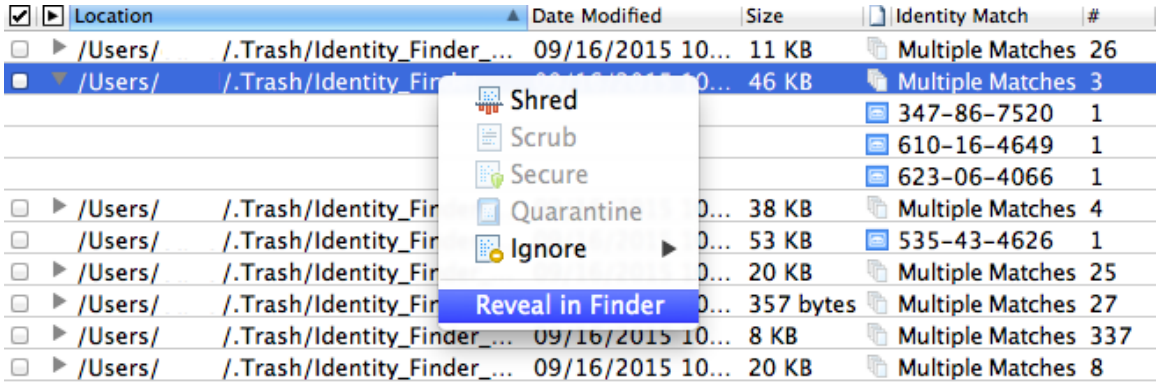
How to Review Results

The Identity Finder results view shows the file location, modified date, size, the type of identity match, and the number of matches. The preview pane on the right shows a portion of the selected document with the results highlighted.



Result examples in this screenshot are sample data and do not indicate real identities.

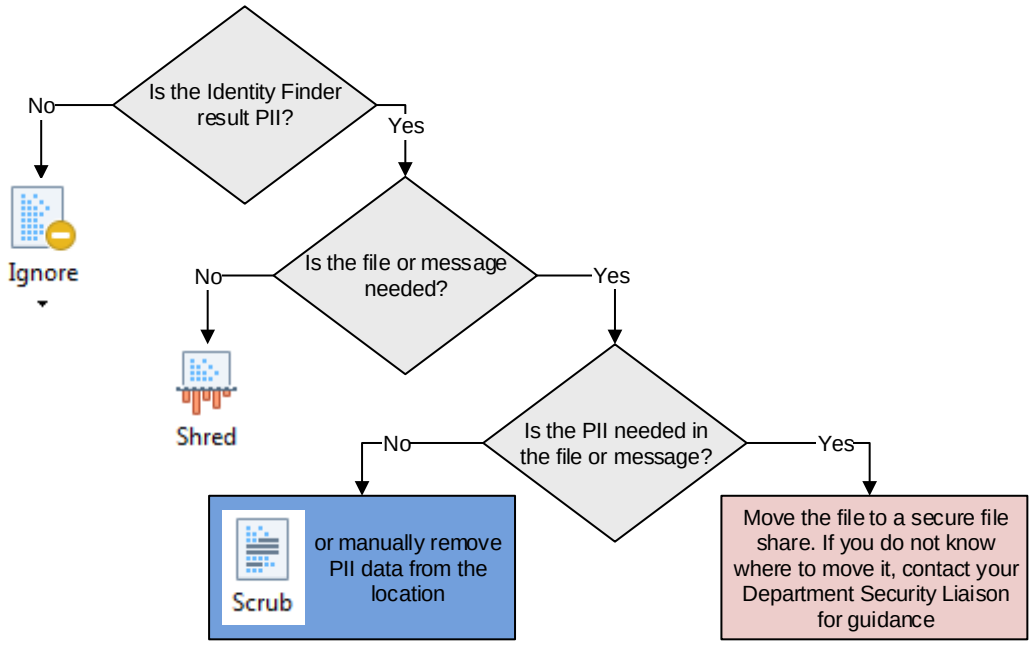
You can right click the result and select **Reveal in Finder** to open the folder containing the file. From there, you can open the file and review it in its entirety before performing an action.



Result examples in this screenshot are sample data and do not indicate real identities.

It is possible to take action on multiple locations at a time. To select more than one location, click the check boxes along the left side of the result.

If you are unsure as to which action you should take on a finding, the below flow chart may assist you in making a decision. **Shred**, **Scrub**, and **Ignore** are explained in detail below.



Shred

The **Shred** action permanently deletes the file containing PII. Files shredded use the secure US Department of Defense data destruction standard known as DOD 5220.22-M. Using Shred removes the file from the results window, as the file no longer exists.

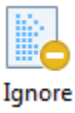
> **Warning:** Files removed with the Shred action are unrecoverable. Be sure the files you shred are no longer needed. If you are unsure about whether a file should be kept, contact your department's Information Security Liaison.

Scrub

The **Scrub** action removes PII from a file while keeping the rest of the data intact, and is a good option to use when the PII is no longer needed but the document itself must be kept. Only some file types can have the scrub action applied to them. Email messages, attachments, PDF files, and files within .zip archives cannot be scrubbed.

Warning: Using this option will replace every character of PII with an X and cannot be undone. If you are unsure if the information should be kept, contact your department's Information Security Liaison.

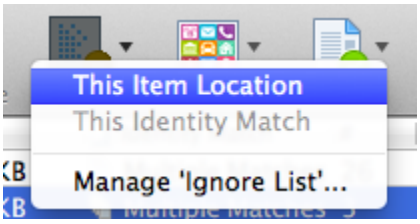
Ignore



If an item found is a false positive or is a file that needs to be kept intact, the result in Identity Finder can be ignored to prevent it from showing up in future scans. Both identity matches and locations can be added to the ignore list. When you ignore a result, you will be prompted to select a reason why you are ignoring it.

Ignore Item Location

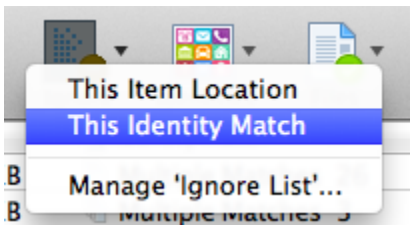
In Identity Finder, a location is a file or email message that contains PII. To ignore the file or email message containing a match, select the result, then then choose **Ignore -> This Item Location**. This location will no longer be reported when subsequent searches are run.



Ignore Identity Match

In Identity Finder, a match is a single finding, such as one individual SSN or credit card number. To ignore the specific identity that was found, for example a test credit card number, select the result, then choose **Ignore -> This Identity Match** from the main menu. This match will no longer be reported in any location when subsequent searches are run.

To ignore the specific identity that was found, for example a test credit card number, select the result, then choose **Ignore -> This Identity Match** from the main menu:



Note: If items are ignored, please note why you chose this option for future reference and review. University IT can work with you to determine the best way to remove PII from your business processes so you do not need to continue collecting it, and provide hard disk encryption software provide an additional layer of data protection.

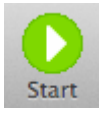
Scheduled scans – what to expect

University IT runs monthly scans of all computers with Identity Finder. You do not need to take any action to begin the scan, but will notice that the Identity Finder application loads in the dock and is minimized. These scans may be scheduled during working hours, as you need to be logged into the computer when the scan starts so the software can search your personal email and files.

When a scheduled scan completes, you are presented with the same results screen as when you run an on demand scan, and can take action on the findings.

On-demand scans

On-demand scans are initiated by you. Identity Finder will only scan files that have been created or changed since the last scan.

On-demand scans are started in the same way as the first scan after installation. Simply click the 

button in the Identity Finder main window.

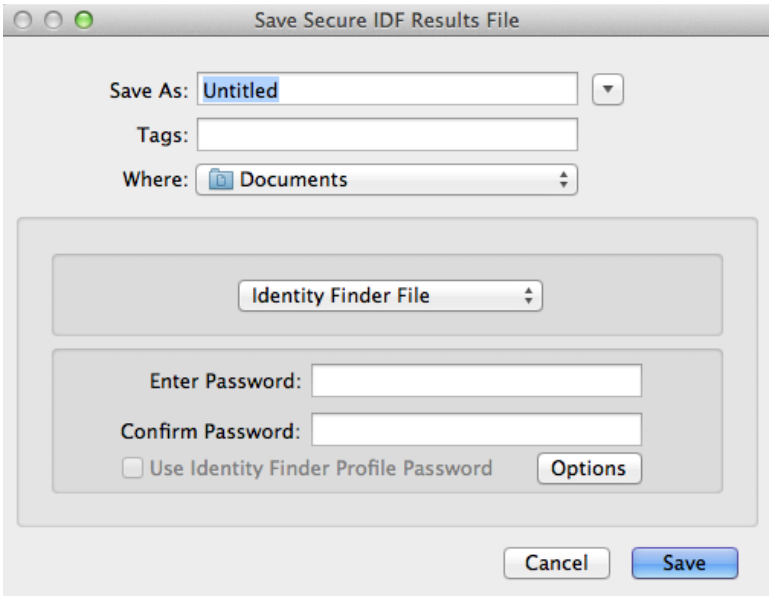
Saving results

If you cannot review all the results in one session, you may want to save the results to continue review at a later time. Results can be saved in three different types of files.

Secure Identity Finder Results File

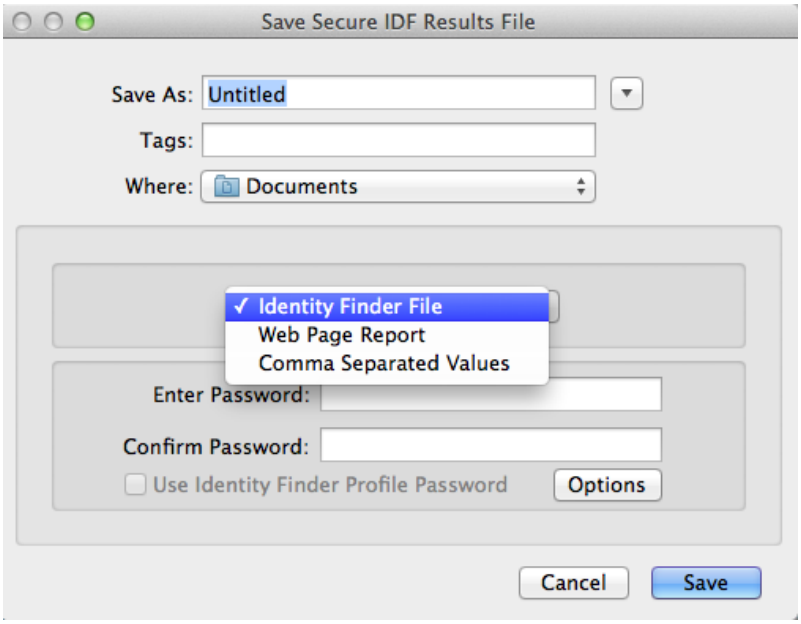
The secure Identity Finder results file is the preferred method for saving results and can be used to save the results for later review and remediation. This is the only results file that can be reopened in Identity Finder.

To save the results in a password protected file, click **Save** from the **File** menu. Choose a location to save the file, and a password to keep it safe. If you forget the password, you will not be able to view the results without re-running a search.



Other Report Types

You can also save the results as a Web Page Report (HTML) or Text (comma separated values) report. These files are not password protected and will not contain the full text of the matches Identity Finder locates – only the file locations and match counts are included. You might want to save the results as one of these files to import the data into Microsoft Excel or to print a report for review with your Departmental Security Liaison.



Contact

- Trouble running the software? Contact the University IT Help Desk.
- Questions about the Identity Finder deployment at the University of Rochester? Email Security and Policy.