End User Identity Finder Guide for Macintosh

Private Information Management at RIT

Information Security Office
Revised December 16, 2011
Contents

Overview ........................................................................................................................................................................... 3
  How will the Private Information Management Initiative affect me? ................................................................. 3
  Frequently Asked Questions ......................................................................................................................................... 3
Scheduled Searches ............................................................................................................................................................. 4
  How do I know when a scheduled search begins? ................................................................................................. 4
  External Devices .............................................................................................................................................................. 4
Introduction to Identity Finder ........................................................................................................................................ 5
  Main Menu ........................................................................................................................................................................ 5
  Identities Menu ................................................................................................................................................................ 6
  Locations Menu ............................................................................................................................................................... 6
  Configuration Menu ......................................................................................................................................................... 7
  Tools Menu ....................................................................................................................................................................... 8
Starting and Stopping an On-Demand Search .................................................................................................................. 8
  How to Start a Search ........................................................................................................................................................ 8
  How to Pause and Resume a Search in Progress ....................................................................................................... 9
  How to Stop a Search ....................................................................................................................................................... 10
  How to Start a Custom On-Demand Search ............................................................................................................ 10
Viewing the Status Window .............................................................................................................................................. 11
  Current Status .................................................................................................................................................................. 11
  Locations Searched Summary ..................................................................................................................................... 12
  Identity Matches Summary ........................................................................................................................................... 12
  How to Display or Hide the Status Window ............................................................................................................. 13
Interacting with Search Results ........................................................................................................................................ 13
  User Decision Making Flow Chart .......................................................................................................................... 14
Shredding (Securely Deleting) Private Information ....................................................................................................... 14
  How to Shred Private Information .......................................................................................................................... 15
  How to Start a Custom On-Demand Shred .............................................................................................................. 15
Scrubbing (Securely Redacting) Private Information ..................................................................................................... 16
Ignoring Search Results ................................................................................................................................................. 16
Launching a File ................................................................................................................................................................. 17
Reports ............................................................................................................................................................................... 17
  Saving Reports .............................................................................................................................................................. 17
Overview

There are a number of federal and state laws governing the safe handling and disposal of Private Information (PI), which is defined as confidential data including Social Security numbers (SSNs), driver’s license numbers, or other account information that could be used for identity theft. These laws mandate special requirements associated with the protection of Private Information. In order to help safeguard the RIT community against identity theft and better comply with these laws, the Private Information Management Initiative (PIMI) program at RIT is implementing tools used to identify and reduce the amount of Private Information contained on RIT-owned computers and external devices connected to the RIT network.

The PIMI program is using Identity Finder (IDF) software to search RIT-owned computers and connected devices for SSNs and other Private Information. Upon completion of a system search, Identity Finder will provide an inventory of all instances of Private Information found on your system. According to RIT policy stated in the updated Information Access & Protection Standard, any Private Information discovered must be redacted, securely erased, securely destroyed, moved to a secure server, or maintained only for approved business reasons.

NOTE: Identity Finder does not handle the secure relocation of Private Information, nor can it determine a business need for Private Information. For help handling Private Information found on your computer or external device, contact your appointed Private Information Steward/Management Representative.

How will the Private Information Management Initiative affect me?

As part of the PIMI program at RIT, Identity Finder software will be installed on your RIT-owned computer. This software provides two types of searches—Scheduled Searches and On-Demand Searches.

- **Scheduled Searches** will occur automatically on a monthly or quarterly basis as determined by the RIT Information Security Office.
- **On-Demand Searches** may be performed at any time. Custom On-Demand Searches can be initiated without launching Identity Finder.

As per the RIT Access & Protection Standard, you will be responsible for remediating all instances of Private Information found on your RIT-owned computer, in your e-mail, and on any other external devices that are used with your RIT-owned computer.

Frequently Asked Questions

A list of Frequently Asked Questions (FAQ) about the PIMI program at RIT and Identity Finder software is available at [http://security.rit.edu/Pim-faq.html](http://security.rit.edu/Pim-faq.html).
Scheduled Searches

Identity Finder will automatically run on a scheduled basis for the continuous protection of Private Information. For questions related to Scheduled Searches, contact your appointed Private Information Steward/Management Representative.

How do I know when a Scheduled Search begins?

When a Scheduled scan initiates, the Identity Finder program will automatically launch in a window on your computer (Figure 1). The Identity Finder icon will pop up on the dock and the window will be minimized. At any time Identity Finder can be maximized by clicking the icon in the Dock. When the scan is completed, another notification will appear (Figure 2).

A search summary appears when the scan is complete (Figure 3). The summary contains the number of identity compromising items on your computer, and the scan results should automatically appear behind it. If you minimize the window, clicking on the Identity Finder icon will maximize it again. You will need to complete remediation at this time. Do not save the report and return to it later.

External Devices

Identity Finder will search any external devices (such as USB flash drives, mp3 players, and smart phones) that are connected to your RIT-owned computer when a Scheduled Search begins.

NOTE: If you do not want Identity Finder to search for Private Information on your external devices, disconnect them prior to the start of a Scheduled Search.
# Introduction to Identity Finder

Identity Finder contains a menu that is a collection of several components, including:

- **Command tabs.** IDF includes five custom Command tabs: **Search, Review, Actions, Identities** and **Locations**; each is described below.
- **Command sets.** Depending on which tab you select, different command sets appear. For example, you must be on the **Search** menu in order to start an Identity Finder search.
- **Contextual commands.** Contextual commands appear for the current task you are performing. For example, **Stop** is not available until you click the **Start** button.

**NOTE:** Some commands are not available at all, such as **Secure, Quarantine, and Recycle.** The RIT Information Security Office has disabled these commands because they are not considered as in scope of the PIMI program.

## Search Menu

The **Search** menu includes the start, stop, resume and pause functions. The status window will display by default in an On-Demand scan, but must be clicked for a Scheduled scan. For more information about protecting Private Information using Identity Finder Actions see “Interacting with Search Results.”

Note: The first three options on the top left of the window contain the same options.

## Review Menu

The **Review** menu allows you to adjust how the scan results are displayed and selected. You can view them by unique identity matches or by source location, and can select or view the entries with this tool. To scroll through selections, you can use the “Previous Match” and “Next Match” options.
Actions Menu

The Actions menu contains the action you would like to apply to an identity match. These are also available in the Identity Finder window, in the top panel. To determine which action to take, see the “User Decision Making Flow Chart.”

Identities Menu

The Identities menu allows you to simultaneously search for identity types. Identity Finder is only enabled to search for four Private Information identity types (as shown with a checkmark to the left of the variable): Social Security numbers, Credit Card numbers, Bank Account numbers, and Driver License numbers. Additional identities are disabled within the application. In other words, you cannot use Identity Finder to search for e-mail addresses, phone numbers, birthdays, or other Private Information.
Locations Menu

The Locations menu includes where Identity Finder will search for Private Information on your system, as shown by the checks. The locations include files and compressed files, e-mails and attachments, browsers, and files located on My Computer.

NOTE: The default Locations Menu is appropriate for compliance with the PIMI program. Customization of this feature is not advised.

The following table lists the locations that identity Finder searches.

Note: The types of searchable locations may vary, based upon the spotlight filters that are installed/enabled.

<table>
<thead>
<tr>
<th>Searchable Locations</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files</td>
<td>Microsoft Excel, PowerPoint, Word, Access, OneNote, Visio, Project</td>
</tr>
<tr>
<td></td>
<td>Adobe Acrobat</td>
</tr>
<tr>
<td></td>
<td>Compressed Zip, z, tar, tar.gz, tar.gz, tar, rar, gzip, bzip, bzip2, and bzip2 files</td>
</tr>
<tr>
<td></td>
<td>Plain Text Files</td>
</tr>
<tr>
<td></td>
<td>ANSI</td>
</tr>
<tr>
<td></td>
<td>Unicode</td>
</tr>
<tr>
<td></td>
<td>Source Code Files</td>
</tr>
<tr>
<td></td>
<td>Cookies</td>
</tr>
<tr>
<td></td>
<td>Instant Messenger Logs</td>
</tr>
<tr>
<td></td>
<td>Rich Text Format</td>
</tr>
<tr>
<td></td>
<td>Web Pages</td>
</tr>
<tr>
<td></td>
<td>Other files (Image Files, Video Files, Music Files, etc.)</td>
</tr>
<tr>
<td>E-mail messages and their attachment files</td>
<td>Microsoft Outlook including Contacts, Calendar, and Tasks</td>
</tr>
<tr>
<td></td>
<td>Outlook Express</td>
</tr>
<tr>
<td></td>
<td>Windows Mail</td>
</tr>
<tr>
<td></td>
<td>Mozilla Thunderbird</td>
</tr>
<tr>
<td></td>
<td>MBOX mail files</td>
</tr>
</tbody>
</table>

NOTE: Identity Finder does not search Web-based e-mail (i.e. Gmail, Yahoo!, or Hotmail).
<table>
<thead>
<tr>
<th>Searchable Locations</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Browsers</td>
<td>• Safari</td>
</tr>
<tr>
<td></td>
<td>• Firefox</td>
</tr>
</tbody>
</table>

**Starting and Stopping an On-Demand Search**

You can start and stop an On-Demand Search at any time. Once you start an On-Demand Search, Identity Finder searches the enabled identities (see "Identities Menu") and locations (see "Locations Menu") you have access to.

**How to Start an On-Demand Search**

Follow these steps to start an On-Demand Search:

1. Open Identity Finder from the Finder, under Applications.
2. Click the Start button in the upper left hand corner or the pulldown option in the Search menu.

The Identity Finder Status window appears, and Identity Finder begins searching for all Private Information matches. Identity Finder will only scan directories and files you have access to. The status window will appear and can be minimized by clicking the Minimize button on the Window menu in Identity Finder.
For more information about the real-time summary of your current search, see “Viewing the Status Window.”

For more information about protecting your Private Information, see “Interacting with Search Results.”

How to Pause and Resume an On-Demand Search in Progress

Pausing a search may be beneficial if you need to interact with a certain result and you find incoming results distracting. It is also helpful if you need to temporarily pause Identity Finder because it is affecting the performance of your computer. Follow these steps to pause and resume an On-Demand Search in progress:

1. Start a search.
2. On the Main menu, click the Pause button. Notice that the Start button changes to Resume. This action can also be completed in the Search menu.
3. To resume the search, click the **Resume** button. This action can also be completed in the **Search** menu.

How to Stop an On-Demand Search

Follow these steps to stop an On-Demand Search:

1. Start a Search.

2. On the Main menu, click the **Stop** button. A dialog box appears with a Confirm Stop message.

3. Click **Yes** to stop the search. You will not be able to resume the search from its current location; if you want to be able to resume your search, click the **Pause** button.

How to Start a Custom On-Demand Search

There is an option if you want to scan a specific folder or file without searching the entire machine for Private Information. This feature is not available in the current version of Identity Finder for Mac.

Viewing the Status Window

The Status window displays the current progress of your search. It has two group boxes: **Current Status**, and **Identity Matches Summary**; each is described below.
Current Status

The **Current Status** group box contains the following information:

- **Searching**: name of the location currently being searched.
- **Progress**: percentage complete for the current location type.
- **Overall**: how far into the total number of location types.
- **Locations Containing Identity Matches / Total Locations Searched**:
  - **Locations Containing Identity Matches**: total number of the items searched so far that contain at least one identity match.
  - **Total Locations Searched**: total number of items of all types searched on your machine so far.
- **Total Identities Found**: total number of Identity Matches found so far across all locations.

Identity Matches Summary

The **Identity Matches Summary** group box lists all of the identity types and the specific number of each type.
How to Display or Hide the Status Window

- Click the Status Window button on the Main menu. A green checkmark in the bottom right corner indicates that the status window is visible.

Interacting with Search Results

Identity Finder allows you to "remediate" Private Information within the program. You may "shred" (securely erase a selected file) or "scrub" (securely remove/redact the Private Information from a document). You should not need technical support or additional software tools to remediate the Private Information found on your computer or attached external devices.

After a search is completed, you must take action on the results.

NOTE: Identity Finder may find your own Private Information on your computer (typically in copies of tax returns, old resumes, forms, etc.). Please redact or remove your own Private Information from your computer to safeguard it.
User Decision Making Flow Chart

Use the decision making flowchart below to determine the appropriate remediation action for Private Information found on your computer or attached external devices.

- To ignore a file, see “Ignoring Search Results.”
- To shred a file, see “Shredding (Securely Deleting) Private Information.”
- To scrub a file, see “Scrubbing (Securely Redacting) Private Information.”

Shredding (Securely Deleting) Private Information

A file (or data) doesn’t get permanently erased from your computer by simply deleting it. Instead, it goes to your Recycle Bin. Even when the Recycle Bin is emptied, file remnants still remain on your
computer. In addition, data recovery techniques provide the ability to recover deleted files with common tools. In order to securely delete Private Information from your computer, you need to use Identity Finder’s shred tool.

**How to Shred Private Information**

The **Shred** action securely deletes the file containing PI from the local machine. Files and folders can also be shredded without Identity Finder being open. Once you click the **Shred** option, you will need to click “Yes” in order to dispose of the document.

**NOTE: A file is unrecoverable after shredding is performed!**

After you have completed this, Identity Finder will notify you that the document has been shredded.

**How to Start a Custom On-Demand Shred**

There is an option if you want to scan a specific folder or file without searching the entire machine for Private Information. This feature is not available in the current version of Identity Finder for Mac.

**Scrubbing (Securely Redacting) Private Information**

The **Scrub** action replaces PI with ‘X’s. Scrub is also known as redact.
Note: The scrub option is not available for all file types.

Ignoring Search Results

The Ignore action flags the selected file or identity match as a false positive. This action must be verified as a false positive by the Information Security Office before it is actually excluded.

Several options are available in the Ignore drop-down menu.

- **This Item Location** ignores all PI matches found by IDF in the file location.
- **This Identity Match** ignores all instances of the specific PI match on your computer.
- **Manage ‘Ignore List’** allows you to edit a list of all ignored matches.

Launching a File

In order to review the PI within the file, click an identity match in the location column to open the directory in which the file is located.
Reports

Identity Finder allows you to generate a report that contains an analysis of your search results. This includes summary information and totals for the number and types of identity matches that were found, as well as the locations containing those matches.

Saving Reports

The scan results may contain files you are unsure how to remediate or need to keep for a business reason. These additional items remaining from the scan must be reported to your Private Information Management technical and/or business representative to determine the reason for keeping the information and how to properly remediate it. Relocating the information to a secure server is a possible solution.

To save a report, click the Save As icon in the Application menu (Figure 11. The Save As dialog box will open. Select Web Page Report (HTML File), then select the folder location and filename for the report.

Note: Reports should be saved as IDF_[username]_[date].html in a Web Page Report.