Rochester Institute of Technology
Information Security Office

End User Identity Finder Guide for Windows

Private Information Management at RIT

identityfinder

Information Security Office
Revised December 10, 2009

Table of Contents

Rochester Institute of Technology
Information Security Office

End User Identity Finder Guide for Windows

Private Information Management at RIT

Overview

There are a number of federal and state laws governing safe handling and disposal of Private Information (PI). Private Information is defined as data that is confidential, could be used for identity theft, and has additional requirements associated with its protection.

In order to help safeguard the RIT community against identity theft and help RIT comply with these laws, the Private Information Management at RIT program uses tools to identify and reduce the amount of PI contained on computers that connect to the RIT network.

Private Information Management at RIT will use software called Identity Finder (IDF) to scan RIT-owned computers and identify PI. Private Information discovered must be modified, deleted securely, moved to a secure server, or maintained only for an approved business reason. Identity Finder does not handle the secure relocation nor can it determine a business need for Private Information. In order to perform these actions, contact your appointed Private Information Management business and/or technical representative.

A Frequently Asked Questions document is available at http://security.rit.edu/Pim-faq.html.

How will Private Information Management at RIT Affect Me?

- Identity Finder software will be installed on your RIT-owned computer
    - Scheduled scans will occur automatically on a weekly basis
        - After an initial cleanup, scans will occur on a monthly basis
    - On-demand scans and remediation may be performed by you at any time
- You will be responsible for remediating all instances of PI found on your computer and any other endpoint devices (such as thumb drives, or external drives) that you use.

Scanning

There are two types of scans. A Scheduled scan is based on a policy set and scheduled by the Information Security Office. An On-Demand scan is launched by the user at any time.

Scheduled Scan

When a Scheduled scan initiates, the Identity Finder icon appears in the Windows System Tray and a taskbar notification will appear above it (Figure 1). Identity Finder is minimized during the scan. At any time Identity Finder can be maximized by clicking the icon in the System Tray. When the scan is completed another taskbar notification will appear (Figure 2).

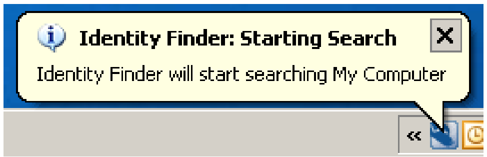

Identity Finder: Starting Search
Identity Finder will start searching My Computer

Figure 1: Search Start Notification

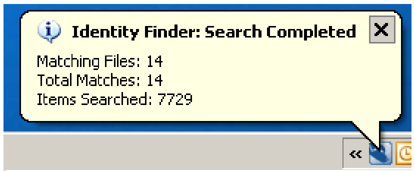
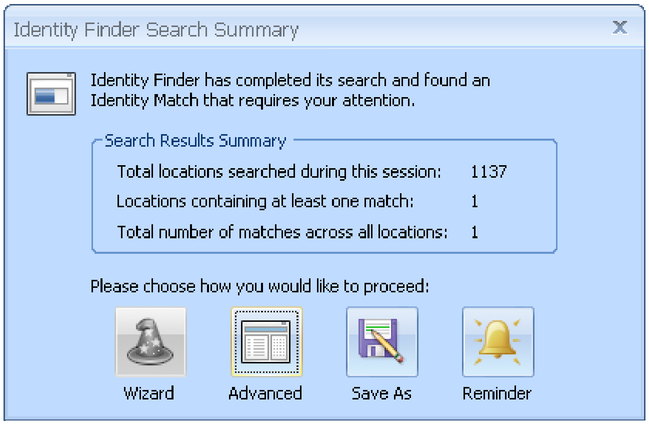

Identity Finder: Search Completed
Matching Files: 14
Total Matches: 14
Items Searched: 7729

Figure 2: Search Completed Notification



Identity Finder Search Summary

Identity Finder has completed its search and found an Identity Match that requires your attention.

Search Results Summary

Total locations searched during this session: 1137
Locations containing at least one match: 1
Total number of matches across all locations: 1

Please choose how you would like to proceed:

Figure 3: Search Summary

A search summary appears when the scan is complete (Figure 3). The summary contains options for you to decide to start remediating now or later. Click the **Advanced** button to view the scan results and begin remediation. If you are currently too busy, click the **Reminder** button and choose a time during the day to remediate your scan results.

Predefined Settings

The Information Security Office controls the end user settings through policies on the server. Default settings are highlighted in the Identity Finder application. Identity Finder has five ribbons of settings: Main, Identities, Locations, Configuration, and Tools.

- The Main ribbon includes the start, stop, and pause functions, as well as filtering, status, and remediation actions. The status window (Figure 5) will display by default in an On-Demand scan, but must be clicked for a Scheduled scan.
- The Identities ribbon includes the types of identity information being searched. Private Information Management at RIT is focusing on locating Social Security Numbers, Credit Card Numbers, Bank Account information, and Driver's license numbers.
- The Locations ribbon includes where Identity Finder will search for identity information. The current settings scan My Computer including removable media, Outlook E-mail and Attachments, Web Browser data, and the Registry, on your machine. IDF scans all types of files including compressed files such as zip.
- The Configuration ribbon includes the User Guide links to Identity Finder's online help page. Additional items on this page will not be used in this program.
- The Tools ribbon contains additional methods of securing information, but they are out of scope for the Private Information Management at RIT Program.

On-Demand Scan

To run a scan manually, open Identity Finder from the desktop icon or Start Menu. Before pressing the start button to initiate the scan you may wish to review the predefined settings. Once pressing the start button (Figure 4), Identity Finder will only scan directories and files you have access to. The status window will appear (Figure 5) and can be minimized by clicking the Status Window button on the Main ribbon in Identity Finder.

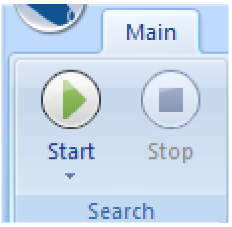
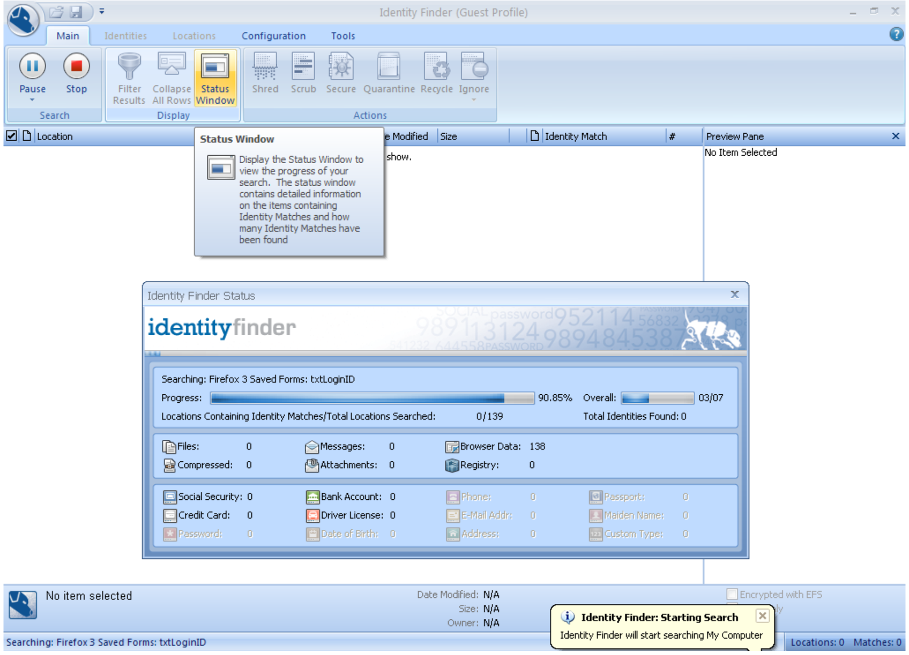


Figure 4: Start



Status Window

Display the Status Window to view the progress of your search. The status window contains detailed information on the items containing Identity Matches and how many Identity Matches have been found

show.

No Item Selected

Identity Finder Status

identityfinder

Searching: Firefox 3 Saved Forms: txtLoginID

Progress: 90.85% Overall: 03/07

Locations Containing Identity Matches/Total Locations Searched: 0/139 Total Identities Found: 0

Files:	0	Messages:	0	Browser Data:	138		
Compressed:	0	Attachments:	0	Registry:	0		
Social Security:	0	Bank Account:	0	Phone:	0	Passport:	0
Credit Card:	0	Driver License:	0	E-Mail Addr:	0	Maiden Name:	0
Password:	0	Date of Birth:	0	Address:	0	Custom Type:	0

No item selected

Date Modified: N/A
Size: N/A
Owner: N/A

□ Encrypted with EFS

Identity Finder: Starting Search
Identity Finder will start searching My Computer

Searching: Firefox 3 Saved Forms: txtLoginID

Locations: 0 Matches: 0

Figure 5: Scan in progress displaying the Status Window

Custom On-Demand Scan

Additionally, there is an option if you want to scan a specific folder or file without searching the entire machine for Private Information. Right-click on the file or folder you want to scan. In the menu you should see an Identity Finder menu with the Identity Finder icon. Expand the menu and click the search option (Figure 6). The Identity Finder application will launch and begin to scan just as an On-Demand scan.

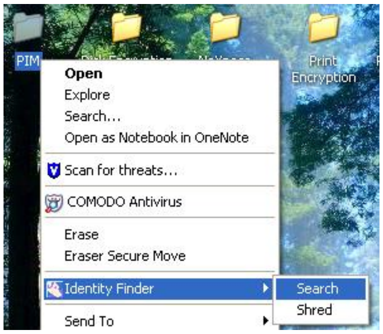
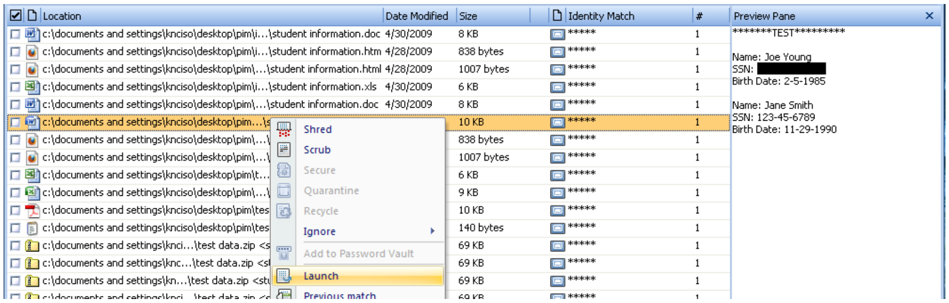


Figure 6: Scan a specific location

Remediation

After a scan, you must take action on the results. The identity matches are masked to prevent Private Information being displayed by Identity Finder.

- In order to review the PI within the file, right-click a location and select **Launch** to open the file or **Open File Location** to open the directory in which the file is located (Figure 7).



☑	Location	Date Modified	Size	Identity Match	#
□	c:\documents and settings\knciso\desktop\pim\i…\student information.doc	4/30/2009	8 KB	*****	1
□	c:\documents and settings\knciso\desktop\pim\i…\student information.htm	4/28/2009	838 bytes	*****	1
□	c:\documents and settings\knciso\desktop\pim\…\student information.html	4/28/2009	1007 bytes	*****	1
□	c:\documents and settings\knciso\desktop\pim\i…\student information.xls	4/30/2009	6 KB	*****	1
□	c:\documents and settings\knciso\desktop\pim\…\student information.doc	4/30/2009	8 KB	*****	1
□	c:\documents and settings\knciso\desktop\pim…\s		10 KB	*****	1
□	c:\documents and settings\knciso\desktop\pim\…\		838 bytes	*****	1
□	c:\documents and settings\knciso\desktop\pim\…\		1007 bytes	*****	1
□	c:\documents and settings\knciso\desktop\pim\t…		6 KB	*****	1
□	c:\documents and settings\knciso\desktop\pim\…\		9 KB	*****	1
□	c:\documents and settings\knciso\desktop\pim\tes		10 KB	*****	1
□	c:\documents and settings\knciso\desktop\pim\tes		140 bytes	*****	1
□	c:\documents and settings\knci…\test data.zip <s		69 KB	*****	1
□	c:\documents and settings\knc…\test data.zip <st		69 KB	*****	1
□	c:\documents and settings\kn…\test data.zip <stu		69 KB	*****	1
□	c:\documents and settings\knci…\test data.zip <s		69 KB	*****	1

Preview Pane

*******TEST*********

Name: Joe Young
SSN: [redacted]
Birth Date: 2-5-1985

Name: Jane Smith
SSN: 123-45-6789
Birth Date: 11-29-1990

Figure 7: Launch a file

User Decision Making Flow Chart

Use the decision making flowchart below to determine the appropriate remediation action.

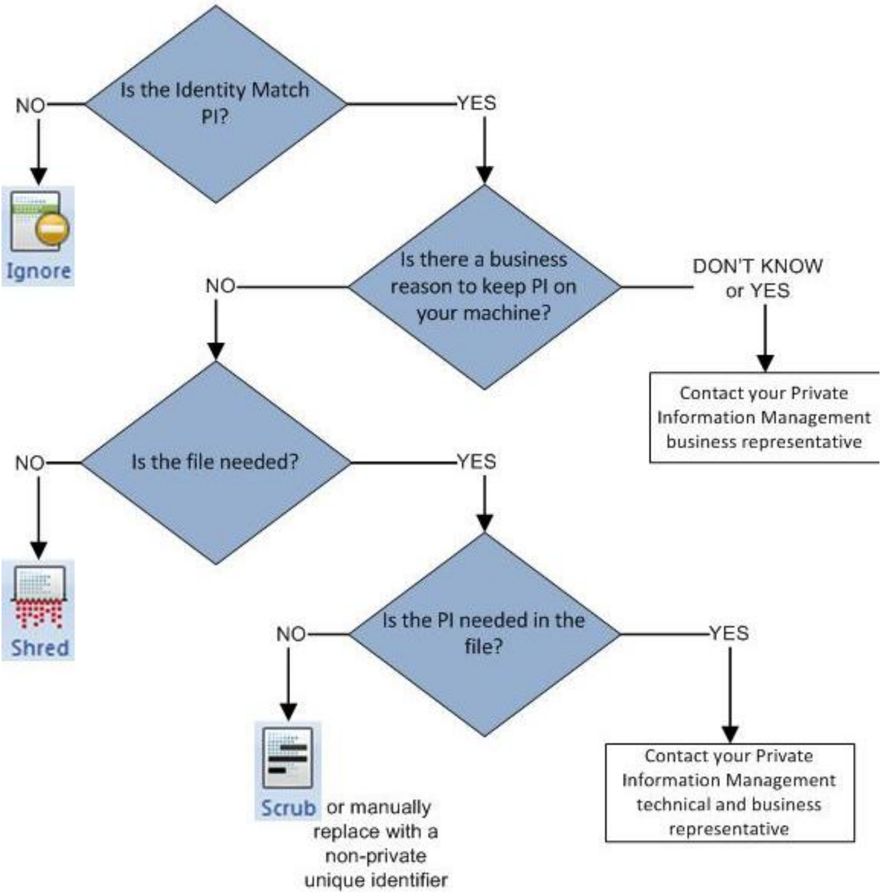
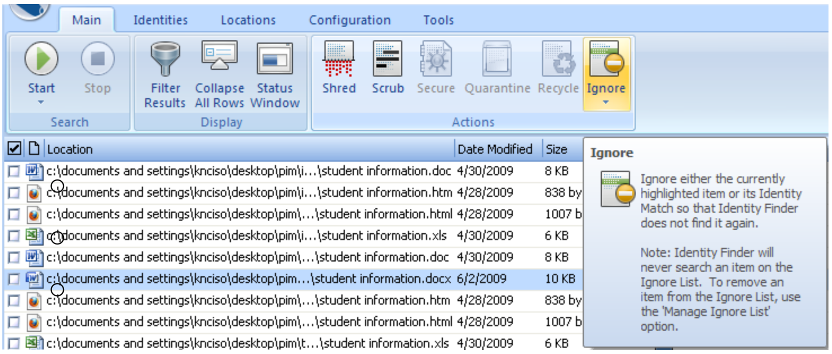

Is the Identity Match PI?
NO
YES
Ignore
Is there a business reason to keep PI on your machine?
NO
DON'T KNOW or YES
Contact your Private Information Management business representative
Is the file needed?
NO
YES
Shred
Is the PI needed in the file?
NO
YES
Scrub or manually replace with a non-private unique identifier
Contact your Private Information Management technical and business representative

Figure 8: User Decision Flow Chart

Actions

Performing an action on PI will remove the row from Identity Finder. In Identity Finder you can ignore, shred, or scrub a file containing PI. Additionally, you can save a report in Identity Finder to discuss with your Private Information Management business representative.

- The **Ignore** action flags the 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.



☑	Location	Date Modified	Size
□	c:\documents and settings\knciso\desktop\pim\i…\student information.doc	4/30/2009	8 KB
□	c:\documents and settings\knciso\desktop\pim\i…\student information.htm	4/28/2009	838 by
□	c:\documents and settings\knciso\desktop\pim\…\student information.html	4/28/2009	1007 b
□	c:\documents and settings\knciso\desktop\pim\i…\student information.xls	4/30/2009	6 KB
□	c:\documents and settings\knciso\desktop\pim\…\student information.doc	4/30/2009	8 KB
□	c:\documents and settings\knciso\desktop\pim…\student information.docx	6/2/2009	10 KB
□	c:\documents and settings\knciso\desktop\pim\…\student information.htm	4/28/2009	838 by
□	c:\documents and settings\knciso\desktop\pim\…\student information.html	4/28/2009	1007 b
□	c:\documents and settings\knciso\desktop\pim\t…\student information.xls	4/30/2009	6 KB

Ignore

Ignore either the currently highlighted item or its Identity Match so that Identity Finder does not find it again.

Note: Identity Finder will never search an item on the Ignore List. To remove an item from the Ignore List, use the 'Manage Ignore List' option.

Figure 9: Ignore Action

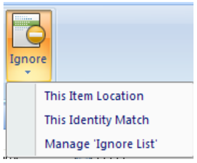
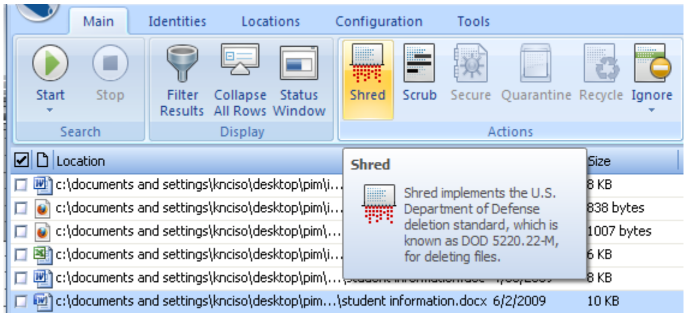


Figure 10: Ignore Action options

- ○ **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 (Figure 10).

- 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 (Figure 6).
  The file is unrecoverable after this action is performed!



Shred

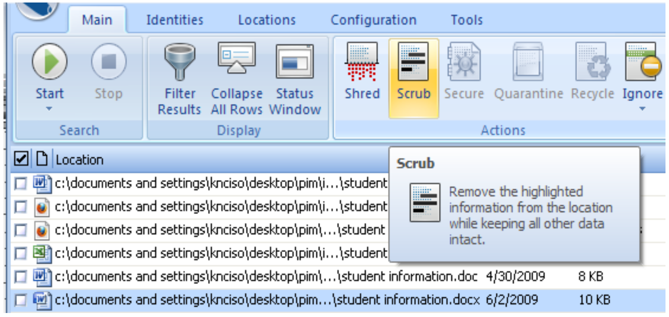
Shred implements the U.S. Department of Defense deletion standard, which is known as DOD 5220.22-M, for deleting files.

☑	Location		Size
□	c:\documents and settings\knciso\desktop\pim\i...		8 KB
□	c:\documents and settings\knciso\desktop\pim\i...		838 bytes
□	c:\documents and settings\knciso\desktop\pim\...		1007 bytes
□	c:\documents and settings\knciso\desktop\pim\i...		6 KB
□	c:\documents and settings\knciso\desktop\pim\...		8 KB
□	c:\documents and settings\knciso\desktop\pim...\student information.docx	6/2/2009	10 KB

Figure 11: Shred Action

- The **Scrub** action replaces the PI with ‘X’s. Scrub is also known as redact.
- The following text file types can be scrubbed:
  - ○ 1st;asm;asp;aspx;bat;btm;c;cc;cmd;cpp;cs;css;cxx;def;dic;h;hpp;hxx;idl;idq;inc;inf;ini;inx;java;js;jsl;log;me;pl;rc;reg;rels;snippet;text;txt;url;vbs;wtx;xml;xsl
  - ○ Microsoft Office files

  The PI is unrecoverable after this action is performed!



Scrub

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

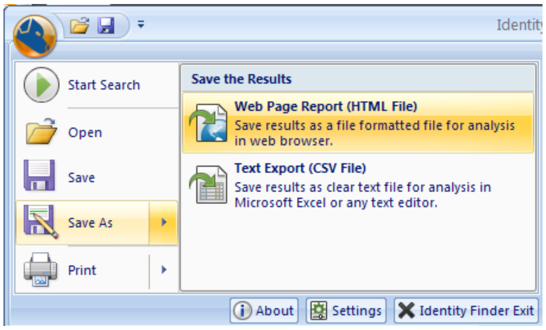
☑	Location		
□	c:\documents and settings\knciso\desktop\pim\i...\student		
□	c:\documents and settings\knciso\desktop\pim\i...\student		
□	c:\documents and settings\knciso\desktop\pim\...\student		
□	c:\documents and settings\knciso\desktop\pim\i...\student		
□	c:\documents and settings\knciso\desktop\pim\...\student information.doc	4/30/2009	8 KB
□	c:\documents and settings\knciso\desktop\pim...\student information.docx	6/2/2009	10 KB

Figure 12: Scrub Action

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.

*Note: Reports should be saved as **IDF_[username]_[date].html**.*



Web Page Report (HTML File)
Save results as a file formatted file for analysis in web browser.

Text Export (CSV File)
Save results as clear text file for analysis in Microsoft Excel or any text editor.

Figure 13: Save As