Identity Finder 3 Documentation
# Table Of Contents

Introduction to Identity Finder .................................................................................................................. 1  
Overview ....................................................................................................................................................... 1  
Identity Finder Editions ............................................................................................................................... 2  
Trial Edition Limitations ............................................................................................................................... 3  
System Requirements, Installation, Uninstallation ...................................................................................... 4  
Minimum Technical Requirements ............................................................................................................... 4  
Installation Instructions .............................................................................................................................. 5  
Activation ...................................................................................................................................................... 6  
Overview ...................................................................................................................................................... 6  
Activating automatically over the Internet ................................................................................................. 7  
Activating manually via E-Mail .................................................................................................................... 10  
Troubleshooting .......................................................................................................................................... 14  
How to Uninstall .......................................................................................................................................... 18  
Quick Start, Tutorials, and Step by Step Wizards ..................................................................................... 19  
Getting Started ........................................................................................................................................... 19  
Tooltips ....................................................................................................................................................... 24  
Tutorial ......................................................................................................................................................... 25  
Step by Step Wizards .................................................................................................................................. 26  
What are Identity Finder Wizards? ............................................................................................................... 26  
Startup Wizard ............................................................................................................................................ 27  
What is the Startup Wizard? ......................................................................................................................... 27  
Automatic Searching Using AnyFind .......................................................................................................... 28  
Automatic Searching Using AnyFind Worldwide ....................................................................................... 29  
Unique Searching Using Your Personal Information .................................................................................. 30  
Where to Search .......................................................................................................................................... 32  
Where to Search .......................................................................................................................................... 32  
File Locations .............................................................................................................................................. 32  
Finalization ................................................................................................................................................... 33  
Results Wizard ............................................................................................................................................. 34  
What is the Results Wizard? ......................................................................................................................... 34  
Loading an Ignore List with Results Wizard ............................................................................................. 38  
Protecting Windows Internet Explorer with Results Wizard .................................................................. 39  
Securing Internet Explorer Hidden Web Data ............................................................................................ 39  
Shredding Internet Explorer Hidden Web Data (AutoComplete Data) .................................................... 39  
Protecting Firefox with Results Wizard .................................................................................................... 40  
Securing Firefox Passwords ....................................................................................................................... 40  
Shredding Firefox Hidden Web Data .......................................................................................................... 40  
Protecting the Windows Registry with Results Wizard ........................................................................... 41  
Protecting Microsoft Outlook with Results Wizard .................................................................................. 42  
Securing Outlook with a Password ............................................................................................................. 42  
Shredding Outlook E-Mails and Attachments ............................................................................................. 42  
Protecting Microsoft Office Files with Results Wizard .......................................................................... 43  
Protecting Adobe Acrobat PDF Files with Results Wizard ...................................................................... 44  
Protecting Compressed Files with Results Wizard .................................................................................. 45  
Protecting Text Based and Other Files with Results Wizard ................................................................... 46  
Scheduling Identity Finder to Run Weekly with Results Wizard ............................................................... 47  
What Personal Information to Search For .................................................................................................. 48  
Identity Match Types .................................................................................................................................. 48
Table Of Contents

What are Identity Match Types? ................................................................................................. 48
Credit Card Numbers .................................................................................................................. 49
Bank Account Numbers ............................................................................................................. 50
Social Security Numbers ........................................................................................................... 51
Passwords ................................................................................................................................... 52
Dates of Birth .............................................................................................................................. 53
Driver’s Licenses ......................................................................................................................... 54
Personal Addresses .................................................................................................................... 55
Passport Numbers ....................................................................................................................... 56
Telephone Numbers ..................................................................................................................... 57
Employee IDs .............................................................................................................................. 58
Mother’s Maiden Names ............................................................................................................. 59
User Defined Types ..................................................................................................................... 60
Australia Tax File Number .......................................................................................................... 62
Canada Social Insurance Number .............................................................................................. 63
United Kingdom National Insurance Number ............................................................................ 64
United Kingdom National Health Service Number .................................................................... 65
Using AnyFind for Automatic Searching .................................................................................. 66
What is Automatic Searching with AnyFind? ........................................................................... 66
Enabling AnyFind ........................................................................................................................ 67
Using Unique Searching ............................................................................................................ 69
What is Unique Searching? ........................................................................................................ 69
Advantages of Unique Searching ............................................................................................... 70
Finding Personal Information with Unique Searching ............................................................... 71
Adding and Removing Unique Identities ................................................................................... 73
What is the Include List? ............................................................................................................. 75
Where to Search for Personal Information .............................................................................. 77
File Locations ............................................................................................................................. 77
What are File Locations? ............................................................................................................ 77
Custom Folder List ....................................................................................................................... 78
Custom Folder List [Enterprise] .................................................................................................. 79
My Documents and Settings Folders ......................................................................................... 81
My Computer ............................................................................................................................... 82
Searching Multiple Remote Computers Enterprise ..................................................................... 83
Home and Office Files ................................................................................................................ 85
What are Home and Office Files? ............................................................................................... 85
Files ........................................................................................................................................... 86
File types searchable by Identity Finder: .................................................................................... 86
Compressed Files ....................................................................................................................... 87
E-Mails ......................................................................................................................................... 88
What are E-Mails? ....................................................................................................................... 88
Messages ......................................................................................................................................... 89
Attachments ................................................................................................................................. 90
System Areas ............................................................................................................................... 91
What are System Areas? ............................................................................................................. 91
Hidden Web Data ........................................................................................................................ 92
Windows Registry ....................................................................................................................... 93
Finding Personal Information ................................................................................................... 94
Starting a Search .......................................................................................................................... 94
Customizing Your Search .......................................................................................................... 94
### Table Of Contents

- What to Search For .................................................................................................................. 94
- Where to Search ...................................................................................................................... 94
- Initiating a Search .................................................................................................................... 95
- Pausing or Stopping a Search ................................................................................................. 96
- Pausing and Resuming a Search in Progress ........................................................................ 96
- Stopping a Search in Progress .................................................................................................. 97
- Reviewing Results ................................................................................................................... 98
- Using the Previous and Next Buttons ..................................................................................... 98
- Anatomy of the Results View .................................................................................................. 99
- Expanding and Collapsing Rows ............................................................................................. 101
- Filtering Results ..................................................................................................................... 102
- What is Filtering? .................................................................................................................... 102
- Resetting Your Filter .............................................................................................................. 103
- Using the Preview Pane .......................................................................................................... 104
- How to Use the Preview Pane .................................................................................................. 104
- Seeking Through Highlighted Matches .................................................................................... 105
- Working with the Status Window ........................................................................................... 106
- Anatomy of the Status Window .............................................................................................. 106
  - Current Status ..................................................................................................................... 106
  - Total Locations Searched ...................................................................................................... 106
  - Total Identity Matches ......................................................................................................... 106
  - Buttons ................................................................................................................................ 107
- Hiding and Compacting the Status Window .......................................................................... 108
- Showing and Hiding ................................................................................................................. 108
- Compacting and Expanding ..................................................................................................... 108
- Progress Bar ............................................................................................................................. 109
- Masking (Hiding) Passwords ................................................................................................... 110
- Hiding Matches from Result View ......................................................................................... 110
- Advantages of Masking Passwords ......................................................................................... 111
- Saving, Opening, and Printing Results .................................................................................... 112
- Saving Results .......................................................................................................................... 112
  - Web Page Report: ............................................................................................................... 113
  - Text Export: ......................................................................................................................... 114
  - Options: ............................................................................................................................... 115
- Opening Results ...................................................................................................................... 117
- Printing Results ....................................................................................................................... 119
- Protecting Personal Information ............................................................................................... 120
- Reminder for Taking Actions on Your Identity Matches ............................................................. 120
- Securing Identity Matches ...................................................................................................... 121
  - Securing Identity Matches: Overview .................................................................................. 121
  - Securing Microsoft Office Files with Encryption .................................................................. 122
  - Securing Compressed Files .................................................................................................. 124
  - Securing Adobe Acrobat PDF Files ...................................................................................... 126
  - Securing Text Based and Other Files Inside Zip (Encrypt) .................................................. 128
  - Securing Microsoft Outlook with Password ........................................................................ 131
  - Securing Firefox with a Master Password ........................................................................... 133
  - Saved Passwords .................................................................................................................. 133
  - Saved Forms .......................................................................................................................... 134
  - Securing Microsoft Internet Explorer (IE) ............................................................................ 135
- Shredding Identity Matches ..................................................................................................... 136
Table Of Contents

Using Permanent Shredding................................................................................................................. 136
Advantages of Shredding.......................................................................................................................... 138
What is DOD 5220.22-M?......................................................................................................................... 138
Recycling Identity Matches...................................................................................................................... 139
Using Windows Recycle to Delete Files.................................................................................................. 139
Disadvantages to Recycle......................................................................................................................... 140
Quarantining Identity Matches ................................................................................................................ 141
Quarantining Files with Identity Matches................................................................................................ 141
Opening Identity Matches ....................................................................................................................... 143
How to Open Results in Associated Application..................................................................................... 143
Working with Results in Associated Application .................................................................................... 144
Ignoring Identity Matches and Locations .............................................................................................. 145
What is the Ignore List? ............................................................................................................................ 145
Ignoring Results ....................................................................................................................................... 147
Ignoring an Identity Match ....................................................................................................................... 148
Ignoring Locations on Your Computer .................................................................................................... 149
Ignoring a Location ................................................................................................................................... 150
Advanced Settings to Customize Your Experience .................................................................................. 151
What are Identity Finder Settings? .......................................................................................................... 151
General Settings ...................................................................................................................................... 152
Popular Settings Page ............................................................................................................................... 152
Associating Identity Finder with Results Files........................................................................................ 153
Giving Other Programs Priority Over Identity Finder ............................................................................ 154
Resetting Message Box Confirmations .................................................................................................... 155
Scheduling Identity Finder to Automatically Run .................................................................................. 156
Export Scheduled Task Search Settings .................................................................................................. 159
Scheduling a Task Using Your Configuration Settings File ................................................................. 161
Startup/Exit Settings .............................................................................................................................. 162
Scheduling Settings Page ....................................................................................................................... 162
Saving and Loading Personal Information File on Startup and Exit ...................................................... 165
Enabling the Startup Wizard When You Open Identity Finder .............................................................. 166
Enabling Autorecover ............................................................................................................................. 167
Saving Search Settings on Exit .............................................................................................................. 168
Checking for New Versions and Updates .............................................................................................. 169
User Interface Settings ............................................................................................................................ 171
Display Settings Page ............................................................................................................................... 171
Showing the System Tray Icon and Balloon Tips .................................................................................. 172
Enabling Word Wrap in Preview Pane ................................................................................................... 173
Specify the Number of Identity Matches Found and Displayed in each Location ................................. 174
Security Settings ....................................................................................................................................... 176
Security Settings Page .............................................................................................................................. 176
Change Your Saved Password for the Personal Information File .......................................................... 177
Configuring Password Strength Requirements ..................................................................................... 179
Configuring Quarantine Location ........................................................................................................... 180
File Search Settings .............................................................................................................................. 181
File Search Settings Page ....................................................................................................................... 181
Searching Only Common File Types, Filterable File Types, Custom File Type List, or All Files .......... 183
Searching Only Files Less than User Specified Size ............................................................................. 185
Searching Only Files Created/Modified Since User Specified Time .................................................... 186
Searching Only New/Modified Files Since Last Search ......................................................................... 187
Table Of Contents
E‐Mail Search Settings ........................................................................................................................................ 189
E‐Mail Settings Page ........................................................................................................................................ 189
Including Outlook and Exchange in E‐Mail Search .......................................................................................... 190
Searching Remote Mail Folders ....................................................................................................................... 191
Searching All or Only Specified Mail Folders ................................................................................................... 192
Select Outlook and Exchange Folders.............................................................................................................. 193
Include Outlook Express or Windows Mail in E‐Mail Search ........................................................................... 195
Searching Only E‐Mails Created/Modified Since User Specified Time ............................................................ 196
Searching Only New/Modified E‐Mails Since Last Search ............................................................................... 197
Hidden Web Data Search Settings ...................................................................................................................... 199
Hidden Web Data Search Settings Page .......................................................................................................... 199
Include Internet Explorer in Search ................................................................................................................. 200
Include Firefox in Search.................................................................................................................................. 201
Search All Locations for Passwords found in Hidden Web Data ..................................................................... 202
Worldwide Search Settings................................................................................................................................. 203
Worldwide Search Settings Page ..................................................................................................................... 203
Enabling Worldwide Searching ........................................................................................................................ 204
Network Search Settings .................................................................................................................................... 205
Registry Search Settings Page .......................................................................................................................... 205
Allowing Prompt for Network Credentials ...................................................................................................... 206
AnyFind Settings ................................................................................................................................................. 207
AnyFind Settings Page ..................................................................................................................................... 207
Searching for Unformatted Social Security Numbers within Locations .......................................................... 209
Requiring Keywords for Unformatted Social Security Numbers ..................................................................... 210
Requiring a Minimum Amount of Social Security Numbers ............................................................................ 211
Comprehensive Password Searching ............................................................................................................... 212
Logging Settings .................................................................................................................................................. 213
Logging Settings Page ...................................................................................................................................... 213
Enabling Logging .............................................................................................................................................. 215
Enabling Log Security ....................................................................................................................................... 217
To view an encrypted Log: ............................................................................................................................ 217
Tools to Secure Your Identity ................................................................................................................................ 219
What are the Identity Finder Tools? ................................................................................................................... 219
Password Vault Tool ........................................................................................................................................... 221
Managing Passwords ....................................................................................................................................... 221
Adding Passwords from Identity Finder .......................................................................................................... 222
Editing Existing Password Inside the Vault ...................................................................................................... 222
Launching Applications from Your Password Vault ......................................................................................... 222
Masking Passowrds.......................................................................................................................................... 222
Secure File Tool................................................................................................................................................... 223
Open Secure Zip File Tool ................................................................................................................................... 224
Shred Files or Folders Tool ................................................................................................................................. 225
Secure Microsoft Internet Explorer (IE) Tool ...................................................................................................... 226
Shred Microsoft Internet Explorer (IE) Hidden Web Data Tool .......................................................................... 227
Secure Firefox Hidden Web Data Tool ............................................................................................................... 229
Saved Passwords.............................................................................................................................................. 229
Saved Forms..................................................................................................................................................... 229
Shred Firefox Hidden Web Data Tool ................................................................................................................. 230
Licensing, Ordering, and Support .......................................................................................................................... 232
Upgrading from Trial Edition .............................................................................................................................. 232
vi


# Table Of Contents

License Agreement ............................................................................................................................................ 233
  Identity Finder End User License Agreement ......................................................................................... 233
Contacting Velosecure for Support ............................................................................................................... 238
Submitting Feedback to Identity Finder Team ............................................................................................. 239
Hints and Tips .................................................................................................................................................. 240
What Information is Sent over Internet to Identity Finder Servers ......................................................... 240
How Frequently Should You Search Your Data ......................................................................................... 241
What Encryption Does Identity Finder Use ................................................................................................. 242
What is FIPS 140-2 ......................................................................................................................................... 243
What are Secure Items Skipped? .................................................................................................................. 244
Choosing Strong Passwords ....................................................................................................................... 245
Installing Additional Filters ...................................................................................................................... 246
Using the System Tray Icon ....................................................................................................................... 247
Benefits .......................................................................................................................................................... 248
  Quickly search your files, E-Mails, and system areas: ............................................................................. 248
  Locate your personally identifiable information: ...................................................................................... 248
  Securely delete or encrypt your sensitive information: .......................................................................... 248
Configuration Settings Files for Scheduling Tasks ..................................................................................... 249
  Sample .ini file: ......................................................................................................................................... 252
  Scheduling a Task Using Your Configuration Settings File .................................................................... 252
Shredder Technology .................................................................................................................................... 253
Troubleshooting ............................................................................................................................................ 254
  Identity Finder is Not Working Properly .................................................................................................... 254
  Contacting Technical Support .................................................................................................................. 256
Warning Messages .......................................................................................................................................... 257
Glossary .......................................................................................................................................................... cclx
Welcome to Identity Finder's Help content. This help includes information for all editions of Identity Finder and may reference features or functions not available to you.

Identity Finder assists you in preventing identity theft by finding personally identifiable information and providing you with the ability to easily and quickly protect it before it is stolen. You can search many areas of your computer for private information and take action to secure it. The following topics will assist you in getting started and using Identity Finder:

- **Before you begin**
  - Technical Requirements
  - Installation Instructions
  - Upgrading from Trial Version
  - Activation
- **Using Identity Finder**
  - Getting Started
  - Identity Match Types
  - Startup Wizard
  - Results Wizard
  - Settings and Options
  - Anatomy of the Results View
  - Anatomy of the Status Window
  - Identity Finder Tools
- **Where to Search**
  - What are File Locations?
  - What are Home and Office Files?
  - What are E-Mails?
  - What are System Areas?

Have questions, comments, or concerns? You can always reach us by submitting feedback to Identity Finder team.
**Identity Finder Editions**

There are three editions of Identity Finder. Each addition has the same core functionality but with enhanced features and each is licensed differently:

- **Identity Finder Home Edition**: This is a desktop, or workstation, compatible version of the product and runs on Windows Vista, Windows XP with Service Pack 1 (SP1), and Windows 2000 Professional with Service Pack 3 (SP3). It requires an activation code the first time it is executed. It only searches the local machine and does not search across the network.

- **Identity Finder Professional Edition**: This is a desktop, or workstation, compatible version of the product and runs on Windows Vista, Windows XP with Service Pack 1 (SP1), and Windows 2000 Professional with Service Pack 3 (SP3). It requires either an activation code or a license key file that facilitates its deployment across an organization’s infrastructure. It only searches the local machine and does not search across the network.

- **Identity Finder Enterprise Edition**: This is the desktop, or workstation, and server compatible version of the product and runs on Windows Vista, Windows XP with Service Pack 1 (SP1), Windows Server 2003 and Windows 2000 Professional and Server with Service Pack 3 (SP3). It requires either an activation code or a license key file that facilitates its deployment across an organization’s infrastructure. It runs across the network and can search files on network drives.
**Trial Edition Limitations**

Identity Finder Trial Edition provides several benefits for consumers and businesses.

- The first is that you can run Identity Finder for free to determine whether or not personal information exists on your computer and what that personal information is. If Identity Finder finds nothing, you just saved yourself some money. If it does find something, you will know what the information is, but not where it is and have a good reason to upgrade.
- The second benefit to the free Trial Edition is the ability to test the software on your home computer or corporate infrastructure to make sure it meets your personal and IT needs.

The following table shows you the key features unavailable to you in the Free Trial Edition version of Identity Finder.

<table>
<thead>
<tr>
<th>Core Features</th>
<th>Free Trial Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Windows Registry</td>
<td>Disabled</td>
</tr>
<tr>
<td>Display identity matches within files</td>
<td>No locations shown</td>
</tr>
<tr>
<td>Use Preview Pane</td>
<td>Disabled</td>
</tr>
<tr>
<td>Display identity matches within autocomplete web browser data</td>
<td>No locations shown</td>
</tr>
<tr>
<td>Display identity matches within saved web browser passwords</td>
<td>No locations shown</td>
</tr>
<tr>
<td>Display identity matches within E-Mails</td>
<td>No locations shown</td>
</tr>
<tr>
<td>Secure files with encryption</td>
<td>Disabled</td>
</tr>
<tr>
<td>Secure web browsers</td>
<td>Disabled</td>
</tr>
<tr>
<td>Secure E-Mail with encryption</td>
<td>Disabled</td>
</tr>
<tr>
<td>Permanently shred files</td>
<td>Disabled</td>
</tr>
<tr>
<td>Securely delete Hidden Web Data</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
System Requirements, Installation, Uninstallation

Minimum Technical Requirements

Identity Finder Home and Professional Editions require Windows Vista, Windows XP with Service Pack 1 (SP1), and Windows 2000 Professional with Service Pack 3 (SP3) and 50MB of free hard drive space. There are no additional requirements such as minimum amount of RAM or CPU speed. Identity Finder Enterprise Edition requires Windows Vista, Windows XP with Service Pack 1 (SP1), Windows 2000 Professional with Service Pack 3 (SP3) or Server or Windows Server 2003.
To install Identity Finder, run the setup program you downloaded from [www.identityfinder.com](http://www.identityfinder.com). If you obtained your copy of Identity Finder from another source, delete it and download a new copy since Internet activation is required and your version may be outdated or fraudulent and could contain spyware. Once Setup has completed, you can run Identity Finder at any time by selecting the Identity Finder icon in your Programs folder.
Activation

All editions of Identity Finder require activation or licensing in order to upgrade from Trial mode to Full mode. Professional and Enterprise Editions allow activation to be skipped by using a corporate license key. License keys can only be obtained by contacting sales@identityfinder.com. Without a corporate license key, activation is a simple process that either requires Internet access or for you to contact us via E-Mail. Once activated, your version of Identity Finder will never need to be activated again.

NOTE: YOUR PERSONAL INFORMATION IS NEVER SENT OVER THE INTERNET UNLESS YOU CHOOSE TO ENTER IT DURING REGISTRATION.

Overview
Activating automatically over the Internet
Activating manually via E-Mail
Troubleshooting

Overview

The first time you run Identity Finder after successfully competing the installation, you will see the Activation Wizard:

If you are evaluating Identity Finder before making a purchase, choose "Continue in Trial Mode" and click "Next" and then click "Finish." If you have not yet purchased an activation code, you may click the "obtain an activation code by clicking here" link and your web browser will open to the Identity Finder store where you may purchase an activation code. If you have already purchased a code, click "Next" and you will see the following. Notice that the title bar has "Identity Finder Home Edition Activation," if you have purchased an activation code for Home Edition, you should continue. If you purchased an activation code for Professional Edition or Enterprise
Edition, you should stop now, visit the Identity Finder website, and download the proper software. A link the correct edition of the software is included in your purchase receipt.

Activating automatically over the Internet

If you choose to activate Identity Finder over the Internet, copy your activation code from your e-mail receipt into the white field. In this example, our activation code is ABCD1234-ABCD-1234-1234-ABCD1234ABCD however, you should use your personal activation code as this code cannot be used to unlock Identity Finder.
After your code is entered as above, click "Next." At this time, Identity Finder will connect to our secure server to send your activation code and only your activation code to ensure that it is correct and that it has not already been used by someone else. None of your personal information is ever sent to us - not during activation, or at any time. We do not collect personal information about you. Your activation does not send your name, address, or any other information to our servers.

After your code has been validated, you will be taken to the registration screen:
You may choose to enter your contact information so you can receive communications from the Identity Finder team, or you may choose to skip this process.

Once registration is complete (or skipped), you will see the following:
You should now click "Finish" and you may begin using all the features of Identity Finder. If Identity Finder encounters errors during the activation process, please refer to the troubleshooting section.

**Activating manually via E-Mail**

If you choose to activate Identity Finder manually, copy your activation code from your e-mail receipt into the white field. In this example, our activation code is ABCD1234-ABCD-1234-ABCD1234ABCD however, you should use your personal activation code as this code cannot be used to unlock Identity Finder. With this method, Identity Finder will never connect to the Internet or send any information to us in any way.

![Identity Finder Activation Dialog]

After your code is entered as above, click "Activate manually via E-Mail" and a PIN code will appear:
Now you must send an e-mail to activation@identityfinder.com with your Activation code and you PIN code. If you click the "Click here to E-Mail your Activation code and PIN code to activation@identityfinder.com" link, your default e-mail will open (as shown below) and you will only need to click send. If your default e-mail is not configured or you use web-based e-mail such as GMail, Yahoo Mail, Hotmail or AOL mail, you should compose a new e-mail, copy and paste your Activation code and PIN code into that e-mail and send it to activation@identityfinder.com. Please do not send the Activation code and PIN code shown below as they cannot be used to unlock Identity Finder. This code contains no personal information and is simply a unique number specific to your computer.
After you receive a response via e-mail from Identity Finder with your personal, unique response code, copy that response code into the white fields as shown here (do not try to activate your software with the response code 1234 1234 1234 1234 1234, it cannot be used to unlock Identity Finder):
After your code is entered as above, click "Next" and you will see the following:

![Identity Finder Home Edition Registration](attachment://registration.png)

You may choose to enter your contact information so you can receive communications from the Identity Finder team, or you may choose to skip this process. Once you are finished, you will see the following:

![Identity Finder Activation Successful](attachment://activation.png)

Your activation was successful. Thank you for choosing Identity Finder to protect your private personally identifiable information. You may contact support@identityfinder.com for any questions or feedback.

The following features are now accessible to you:

* Find all identity matches on your computer.
* Search custom folders on your computer.
* Securing files using associated application encryption.
* Securing your web browsers.
* Securing E-Mail with encryption.
* Permanently shredding files so they may not be recovered by hackers.
* Secure deletion of hidden web data.
* Shredding of other data on your computer.
* Ability to find identity matches within Windows Registry.
* No more nag screen.
You should now click "Finish" and you may begin using all the features of Identity Finder. If Identity Finder encounters errors during the activation process, please refer to the troubleshooting section.

**Troubleshooting**

If Identity Finder encounters errors during the activation process, you may see one of the following messages.

**Message:** Invalid Activation Code - The Activation code you have entered does not appear to be valid. Please re-check and enter your code again exactly as it appears, including any dashes or spaces without adding any additional characters.

**Reason:** Your activation code was not entered properly.

**Screenshot:**

[Image of invalid activation code]

**Solution:**
Your activation code was not entered exactly as it appeared in your receipt. Please return to your original receipt and use Windows to copy and paste the code directly into Identity Finder. If you are unable to use Windows copy and paste, make sure all of the spaces, digits, letters and dashes are entered exactly as they appear in your receipt.

**Message(s):**
- The Activation Code that you have entered is incorrect. Please check your code, verify that it is valid for Identity Finder Home Edition, and try again or click Back and then continue in Trial mode.
- The Activation Code that you have entered is incorrect. Please check your code, verify that it is valid for Identity Finder Professional Edition, and try again or click Back and then continue in Trial mode.

**Reason:** Your activation code appears to be valid, however it was rejected by the Identity Finder server - most likely because it was used with the wrong edition of Identity Finder.

**Screenshot:**
Solution:
The most common reason for this message is that you are attempting to use an activation code for the wrong edition of Identity Finder. Notice that the title bar in the image above reads, "Identity Finder Home Edition Activation." If you have purchased an activation code for Home Edition, you should check to make sure your code is correct and then try again. If you purchased an activation code for Professional Edition or Enterprise Edition, you should stop now, visit the Identity Finder website, and download the proper software. A link the correct edition of the software is included in your purchase receipt. Similarly, if the title bar reads, "Identity Finder Professional Edition Activation" as shown below, and you have purchased an activation code for Identity Finder Home Edition, please download the correct software.
**Message:** You have exceeded the number of activations that you have purchased.

**Reason:** You have already activated the number of copies of Identity Finder that you have purchased.

**Solution:**
After you activate Identity Finder once for each number of licenses you have purchased, your code is disabled to prevent piracy. If you receive this error even though you have not yet used your full allotment of licenses, it is possible that someone else has used your activation code. In this case, please send an e-mail to support@identityfinder.com and describe the circumstances of the issue. We may be able to reset your activation counter or may need to issue you a new activation code.

---

**Message:** This activation has been blocked.

**Reason:** The activation code you are using has been marked as lost or stolen and is no longer valid.

**Solution:**
If you are the legal owner of this activation code, please send an e-mail to support@identityfinder.com and describe the circumstances of the issue.

---

**Message:** The Activation server could not be reached. Please make sure you are connected to the Internet and that you do not have a firewall blocking Identity Finder. If the problem persists, please activate manually.
**Reason:** Either your computer could not contact the Identity Finder server or the response to your activation request was blocked.

**Solution:**
Check that you are currently connected to the internet by using your web browser to visit http://www.identityfinder.com and another website of your choosing. If you cannot view both sites, you will not be able to use online activation. If you can view both sites, exit the Identity Finder Activation Wizard, reboot, and try again. If the problem persists, try to activate manually or contact support@identityfinder.com

**Message:** The Activation server could not be contacted. Please make sure you are connected to the Internet and that you do not have a firewall blocking Identity Finder. If the problem persists, please activate manually.

**Reason:** Either your computer could not contact the Identity Finder server or the response to your activation request was blocked.

**Solution:**
Check that you are currently connected to the internet by using your web browser to visit http://www.identityfinder.com and another website of your choosing. If you cannot view both sites, you will not be able to use online activation. If you can view both sites, exit the Identity Finder Activation Wizard, reboot, and try again. If the problem persists, try to activate manually or contact support@identityfinder.com

**Message:** There was an unknown error with your Activation, please contact support@identityfinder.com

**Reason:** Identity Finder encountered an error other than those listed above while attempting to activate your software.

**Solution:**
Check that you are currently connected to the internet by using your web browser to visit http://www.identityfinder.com and another website of your choosing. If you cannot view both sites, you will not be able to use online activation. If you can view both sites, exit the Identity Finder Activation Wizard, reboot, and try again. If the problem persists, please contact support@identityfinder.com
How to Uninstall

To uninstall Identity Finder, run the Uninstall application from your Identity Finder programs folder. All Identity Finder files will be deleted, your personal settings removed from the registry, and if you scheduled a task that will be deleted.

Alternatively, you may utilize the Add/Remove Programs feature from Windows' Control Panel.
Quick Start, Tutorials, and Step by Step Wizards

Getting Started

Identity Finder is easy to use. To get started go to the Windows Start Menu, choose Programs, then the Identity Finder group, then Identity Finder:

Once open, you may choose "Start Searching Now" to immediately start your search with the default options (or previously saved options) or continue in Wizard mode by clicking Next:
Quick Start, Tutorials, and Step by Step Wizards

Click Next again to enable **AnyFind**:

Click Next again to enable **Unique Searching Using Your Personal Information** for additional **Identity Match Types**:
Enter any personal information you choose or skip this task by clicking Next again:

Click Next again to search All Files within your My Documents and Settings folder:
Click Next again to confirm all your selections:

Identity Finder will begin searching for all identity matches. A Status Window will appear to show your current status:
You may interact with results as they appear or wait for the results wizard to appear when Identity Finder is complete. When complete you will see a dialog box with your summary results. Click OK with Wizard selected and Identity Finder will begin taking you through the Results Wizard:
**Tooltips**

There are numerous Tooltips throughout Identity Finder to assist you with learning to use the product more effectively and efficiently. If you do not know what a certain button or field is intended to do, try hovering your mouse over the button or field for one to two seconds without any motion. If you still need additional help, open the Help by pressing the F1 key or clicking the help icon on the ribbon.
Tutorial

A five minute Adobe Flash tutorial is available on our website:

http://www.identityfinder.com/demo/
Step by Step Wizards

What are Identity Finder Wizards?

Wizards within Identity Finder assist you in performing tasks more easily. Through a work flow approach, the Wizard will walk you through many options needed to start a search or secure your results step by step. To use a wizard, choose the Wizard button on the Main ribbon and then after you see the drop down menu, choose either Startup Wizard or Results Wizard. Startup Wizard will walk you through setting up a new search and clear all your current findings.

- Startup Wizard
- Results Wizard
Startup Wizard

What is the Startup Wizard?
The Startup Wizard is an easy to use, quick way to begin using Identity Finder. It provides the most common options you will need to configure your search, such as Automatic Searching Using AnyFind, Unique Searching Using Your Information, and Where to Search. By default, you will be prompted to use the Startup Wizard when Identity Finder is opened. There are three options:

- Start Searching Now
- Continue in Wizard Mode
- Skip Wizard and Use Advanced Mode

Start Searching Now: Immediately starts the Identity Finder search using the options you have saved from previous sessions or, if this is your first time running Identity Finder, by using the default options.

Continue in Wizard Mode: Prompts you to answer several questions and then starts the Identity Finder search.

Skip Wizard and Use Advanced Mode: Skips the Wizard and lets you configure Identity Finder using the main interface. This is the most powerful way to configure Identity Finder as all options will be available to you.

You can also initiate the wizard by clicking the "Wizard" button on the Main ribbon. If the Startup Wizard does not open when you launch Identity Finder, you can enable it via the Settings dialog box.
Automatic Searching Using AnyFind

Automatic Searching Using AnyFind will allow you to search for Identity Matches without entering any information. The AnyFind page allows you choose which **Identity Match Types** you want to automatically find without providing any specific personal information. You can enable searching for Credit Card Numbers, Bank Account Numbers, Social Security Numbers, and Passwords. By default all four types are enabled.

You also have the option of choosing whether you want to search for Worldwide personal information using the AnyFind Worldwide Searching feature. This is useful for automatically finding personal information typically stored in additional countries. If you would like to enable AnyFind Worldwide Searching, choose the Yes option and click Next to enter that information on the next page.

When you have completed your selections, click Next to proceed.
Automatic Searching Using AnyFind Worldwide

Automatic Searching Using AnyFind Worldwide will allow you to search for additional Identity Matches without entering any information. The AnyFind Worldwide page allows you choose which Identity Match Types you want to automatically find without providing any specific personal information. You can enable searching for Australia Tax File Numbers, Canada Social Insurance Numbers, United Kingdom National Insurance Numbers, and United Kingdom National Health Service Numbers. By default all four types are disabled:

When you have completed your selections, click Next to proceed.
Unique Searching Using Your Personal Information

Unique Searching Using Your Personal Information will allow you to search for Identity Matches for which you provide personal information.

If you would like to provide personal information to find any of those Identity Match Types, choose the Yes option and click Next to enter that information on the next page.

The next page provides you the option of choosing whether you want to provide unique, specific personal information for eight of the Identity Match Types. You can provide personal information for Dates of Birth, Driver's Licenses, Personal Addresses, Passport Numbers, Telephone Numbers, Employee IDs, and Mother's Maiden Names.

For each piece of personal information you wish to provide, enter it in the appropriate field on the left side of the wizard and then click Add to move the data into the Include List on the right. To enter additional information, repeat this process. When you have entered all the information you desire, click Next to proceed.
For each piece of personal information you wish to provide, enter it in the appropriate field on the left side of the wizard and then click Add to move the data into the Include List on the right. To enter additional information, repeat this process. When you have entered all the information you desire, click Next to proceed.

Note: Identity Finder doesn't simply search for the personal information you enter, but rather it converts that information into multiple formats to increase the likelihood of discovering matches. For example, when you enter 03/12/1972 as a Date of Birth, Identity Finder will match all of the following formats (and others) in any location:

- 03/12/1972
- 03/12/72
- 03-12-1972
- 03-12-72
- Mar. 12, 1972
- March 12, 1972

Note: Identity Finder will also look for any words you enter in various cases so it is not necessary to enter Smith, smith, and SMITH. Any one of these will match all three versions.
Where to Search

Where to Search will allow you to choose the items and locations on your computer where Identity Finder will search for identity matches. There are two options for you to configure: File Locations and Where to Search.

Where to Search

Choose the items and locations on your computer where you would like to search.

- All Files
- E-Mails and Attachments
- Hidden Web Data
- Windows Registry

File Locations

- My Documents and Settings
- My Computer
- Custom Location

Note: If you deselect the "All Files" option in Where to Search, the File Location options will be unavailable as this information is irrelevant since Identity Finder will not be searching files.

When you have completed your selections, click Next to proceed.
Finalization

The Final page of the Startup Wizard displays a summary of all the options you selected. After you confirm your options are correct, click Finish and Identity Finder will begin searching your computer. If you would like to make changes to your selections, click Back.
Results Wizard

What is the Results Wizard?
The Results Wizard is an easy to use, quick way to secure your results using Identity Finder. By default you will be prompted to use the Results Wizard when Identity Finder is finished searching your computer. However, you can also initial the wizard by clicking the "Wizard" button on the Main ribbon any time after your search is complete while there are still results in the Results View.

Note: Only the Result Wizards pages relevant to your results will be displayed as you proceed through the wizard. The Quarantine feature is only available in Professional and Enterprise Editions. Microsoft Access Database files will only be searched in Professional and Enterprise Editions.

Below is the complete set:
Quick Start, Tutorials, and Step-by-Step Wizards

You have Identity Matches in your Internet Explorer Hidden Web Data. What action would you like to take on your Internet Explorer Hidden Web Data (AutoComplete Form Data and Saved Passwords)?

- Shred Selected
- Ignore Selected Locations
- Skip Remaining Items

You have unprotected saved Firefox Passwords. Would you like to enable Firefox's Master Password to secure your password list?

- Yes
- No

You have Identity Matches in your Firefox Hidden Web Data. What action would you like to take on your Firefox Hidden Web Data?

- Shred Selected
- Ignore Selected Locations
- Skip Remaining Items

There is no password on your Microsoft Outlook E-mail Personal Folder. Would you like to add a password to protect it?

- Yes
- No
Quick Start, Tutorials, and Step by Step Wizards

You have Identity Matches in your e-mail messages. What action would you like to take on your e-mail messages?

- Shred Selected
- Ignore Selected Locations
- Skip Remaining Items

You have Identity Matches in your Microsoft Office Files (Word Documents, Excel Spreadsheets, PowerPoint Presentations). What action would you like to take on your Microsoft Office Files?

- Secure Selected
- Quarantine Selected
- Shred Selected
- Ignore Selected Locations
- Recycle Selected
- Skip Remaining Items

You have Identity Matches in your Microsoft Access Database Files. What action would you like to take on your Microsoft Access Database Files?

- Secure Selected
- Quarantine Selected
- Shred Selected
- Ignore Selected Locations
- Recycle Selected
- Skip Remaining Items

You have Identity Matches in your Adobe Acrobat PDF Files. What action would you like to take on your Adobe Acrobat PDF Files?

- Secure Selected
- Quarantine Selected
- Shred Selected
- Ignore Selected Locations
- Recycle Selected
- Skip Remaining Items
Quick Start, Tutorials, and Step by Step Wizards

You have Identity Matches in your Compressed/Zip Files. What action would you like to take on your Compressed/Zip Files?

- Secure Selected
- Quarantine Selected
- Shred Selected
- Ignore Selected Locations
- Recycle Selected
- Skip Remaining Items

You have Identity Matches in other files. What action would you like to take on your other files?

- Secure Selected
- Quarantine Selected
- Shred Selected
- Ignore Selected Locations
- Recycle Selected
- Skip Remaining Items

You have finished using the Results Wizard. Depending on the options you chose for this search, there may still be Identity Matches on your computer. Additionally, as you work, chat, E-Mail, and use the Internet, the information on your computer constantly changes.

To continue protecting your personal information we recommend scheduling Identity Finder to run automatically once per week.

- Schedule a weekly Identity Finder search.
Loading an Ignore List with Results Wizard

The Ignore List page will only appear if you have personal information saved in an Ignore List but did not load the list when you started Identity Finder or have not manually loaded the list from the Settings dialog box.

If you have an Ignore List that has not been loaded, you will see this page:

![Ignore List Wizard](image)

You may filter your results by loading your previously saved Ignore List. It is not currently loaded, would you like to load it now?

- Yes
- No

If you choose to load the Ignore List, all ignored locations and identity matches will be removed from your results view saving you the time of removing them manually. If you select Yes and click Next, you will be prompted to enter your Ignore List password.
Protecting Windows Internet Explorer with Results Wizard

If you have identity matches in your Internet Explorer Hidden Web Data, you will see two Internet Explorer Results Wizard pages: one to Secure your Internet Explorer configuration and one to Shred your current Internet Explorer Hidden Web Data results.

Securing Internet Explorer Hidden Web Data

If you have Internet Explorer Hidden Web Data identity matches and Internet Explorer is configured to save Hidden Web Data, you will see this page:

The page displays your current Internet Explorer settings and allows you to modify them. To secure Internet Explorer by preventing its ability to save AutoComplete data in the future, disable (uncheck) the ability to save (1) AutoComplete Form Data and (2) username and passwords on forms. Note that from this point forward, when you are visiting a merchant's website and enter your personal information to make a purchase, Internet Explorer will not save this information. The downside to this is you will need to retype your personal information every time you visit that site, but this is outweighed by the knowledge that no one can access your personal information via Internet Explorer.

Shredding Internet Explorer Hidden Web Data (AutoComplete Data)

If you have Internet Explorer Hidden Web Data identity matches, you will see this page:

The page allows you to Shred the selected results below it, Ignore the selected locations, or skip this task.
Protecting Firefox with Results Wizard
If you have identity matches in your Firefox Hidden Web Data, you will see two Firefox Results Wizard pages: one to Secure Firefox with a Master Password and one to Shred your current Firefox Hidden Web Data results.

Securing Firefox Passwords
If you have Firefox Saved Passwords, you will see this page:

You have unprotected saved Firefox Passwords. Would you like to enable Firefox’s Master Password to secure your password list?

- Yes
- No

The page allows you to Secure Firefox with a Master Password.

Shredding Firefox Hidden Web Data
If you have Firefox Hidden Web Data identity matches, you will see this page:

You have Identity Matches in your Firefox Hidden Web Data. What action would you like to take on your Firefox Hidden Web Data?

- Shred Selected
- Ignore Selected Locations
- Skip Remaining Items

The page allows you to either Shred the selected results below it, Ignore the selected locations, or skip this task.
Protecting the Windows Registry with Results Wizard

If you have Windows Registry values with identity matches, you will see this page:

You have Identity Matches in your Windows Registry. What action would you like to take on your Windows Registry items?

- Shred Selected
- Ignore Selected Locations
- Skip Remaining Items

The page allows you to either Shred the selected results below it, Ignore the selected locations, or skip this task.
Protecting Microsoft Outlook with Results Wizard
If you have identity matches in Microsoft Outlook, you will see two E-Mail Results Wizard pages: one to Secure your Outlook with a password and one to Shred your E-Mail messages and their attachments.

If you have identity matches in Microsoft Outlook Express or Windows Mail, you will only see the second Results Wizard page below.

Securing Outlook with a Password
If you have an Outlook Personal Folder that you can secure, you will see this page.

The page allows you to Secure Microsoft Outlook with a Password.

Shredding Outlook E-Mails and Attachments
If you have E-Mails and/or Attachments within Microsoft Outlook, Microsoft Outlook Express, or Windows Mail with identity matches, you will see this page:

The page allows you to either Shred the selected results below it, Ignore the selected locations, or skip this task.
Protecting Microsoft Office Files with Results Wizard

If you have Microsoft Office files with identity matches, you will see this page:

The page allows you to either Secure the selected results, Shred the selected results, Recycle the selected results, Quarantine the selected results, Ignore the selected locations, or skip this task. Note: Quarantine is only available in Identity Finder Professional and Enterprise Editions.
Protecting Adobe Acrobat PDF Files with Results Wizard
If you have Adobe Acrobat PDFs with identity matches, you will see this page:

The page allows you to either Secure the selected results, Shred the selected results, Recycle the selected results, Quarantine the selected results, Ignore the selected locations, or skip this task. Note: Quarantine is only available in Identity Finder Professional and Enterprise Editions.
Protecting Compressed Files with Results Wizard

If you have Compressed Files with identity matches, you will see this page:

The page allows you to either Secure the selected results, Shred the selected results, Recycle the selected results, Quarantine the selected results, Ignore the selected locations, or skip this task. Note: Quarantine is only available in Identity Finder Professional and Enterprise Editions.
**Protecting Text Based and Other Files with Results Wizard**

If you have Text Based or Other Files with identity matches, you will see this page:

- Secure Selected
- Quarantine Selected
- Shred Selected
- Ignore Selected Locations
- Recycle Selected
- Skip Remaining Items

The page allows you to either **Secure** the selected results, **Shred** the selected results, **Recycle** the selected results, **Quarantine** the selected results, **Ignore** the selected locations, or skip this task. **Note:** Quarantine is only available in Identity Finder Professional and Enterprise Editions.
Quick Start, Tutorials, and Step by Step Wizards

**Scheduling Identity Finder to Run Weekly with Results Wizard**
The final Results Wizard page will prompt you to Schedule Identity Finder to run weekly. This is extremely important to protect your identity as during each week you are accessing the internet, receiving E-Mails, and modifying files. By default, Identity Finder will search your computer every Saturday night at 11:00pm. You may change this schedule, or the settings for the scheduled search, at any time via the Settings dialog box.

![Results Wizard Page]

You have finished using the Results Wizard. Depending on the options you chose for this search, there may still be Identity Matches on your computer. Additionally, as you work, chat, E-Mail, and use the Internet, the information on your computer constantly changes.

To continue protecting your personal information we recommend scheduling Identity Finder to run automatically once per week.

- [ ] Schedule a weekly Identity Finder search.
What Personal Information to Search For

Identity Match Types

What are Identity Match Types?

Identity Match Types are ways you can store your identity digitally. For example, a password gives you access to a website or your E-Mail; a credit card allows you to buy something; a social security number allows you to sign up for a bank account; a bank account gives you access to your money; your mother’s maiden name or your birth date is how you identify yourself on the phone to certain institutions.

Identity Finder helps you find all these Identity Match Types and more:

- Credit Card Numbers
- Bank Account Numbers
- Social Security Numbers
- Passwords
- Dates of Birth
- Driver’s Licenses
- Personal Addresses
- Passport Numbers
- Telephone Numbers
- Employee IDs
- Mother’s Maiden Names
- User Defined Types
- Australia Tax File Number
- Canada Social Insurance Number
- United Kingdom National Insurance Number
- United Kingdom National Health Service Number
Credit Card Numbers

Identity Finder will locate Credit Card Numbers without requiring you to provide any personal information. It uses the AnyFind proprietary technology to find valid Credit Card numbers, and then assigns an icon to the identity match that represents the specific credit card issuer. If you want to search for only a specific Credit Card Number, you should disable AnyFind and add your credit card to the Unique Identity Include List. Credit Card Numbers can be used to make unauthorized purchases on your behalf, so searching for this Identity Match Type is of critical importance.

By default, Identity Finder will always search for Credit Card Numbers using AnyFind. However, you may customize this behavior.

If you are using the Startup Wizard, you can select or deselect the "Credit Card Numbers (or Debit Card)" option and you can choose to add specific, unique Credit Card Numbers to the search.

If you are not using the Startup Wizard, you can enable or disable AnyFind searching for Credit Card Numbers by clicking the "Credit Card" button on the What to Search For ribbon. When the button has an orange highlight, it is enabled and Identity Finder will use AnyFind searching. You can also Add a Credit Card Number to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon). Within that dialog box, when Credit Card Number is selected in the "Identity Type" drop down box, you can check or uncheck the "Enable Automatic Search for Credit Card" to change your AnyFind settings for Credit Card Numbers. The ribbon button will update automatically to reflect any changes you make here.

Note: When entering a unique Credit Card Number, it must be entered as 13-16 digits with or without spaces, but without dashes or any other characters. For example "4111111111111111" (without the quotes) is valid. However "4111-1111-1111-1111" (without the quotes) is invalid because it contains dashes.
Bank Account Numbers

Identity Finder will locate Bank Account Numbers without requiring you to provide any personal information. It uses the AnyFind proprietary technology to find series of numbers that represent bank accounts. If you want to search for a Bank Account Number containing letters, you should add your specific bank account to the Unique Identity Include List. If you want to search for only a specific Bank Account Number, you should disable AnyFind and add your bank account to the Unique Identity Include List. Bank Account Numbers can be used to gain access to your financial information and conduct transactions on your behalf, so searching for this Identity Match Type is of critical importance.

If you are using the Startup Wizard, you can select or deselect the "Bank Account Numbers" option and you can choose to add specific, unique Bank Account Numbers to the search.

If you are not using the Startup Wizard, you can enable or disable AnyFind searching for Bank Account Numbers by clicking the "Bank Account" button on the What to Search For ribbon. When the button has an orange highlight, it is enabled and Identity Finder will use AnyFind searching. You can also Add a Bank Account Number to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon). Within that dialog box, when Bank Account Number is selected in the "Identity Type" drop down box, you can check or uncheck the "Enable Automatic Search for Bank Account" to change your AnyFind settings for Bank Account Numbers. The ribbon button will update automatically to reflect any changes you make here.

Note: When entering a unique Bank Account Number, it must be entered as 5-30 letters, numbers, dashes or spaces but without any other characters. For example "PB-12345" (without the quotes) is valid. However "#PB-12345" (without the quotes) is invalid because it contains a number sign (#).
What Personal Information to Search For

Social Security Numbers

Identity Finder will locate Social Security Numbers without requiring you to provide any personal information. It uses the AnyFind proprietary technology to find valid Social Security numbers. If you want to search for only a specific Social Security Number, you should disable AnyFind and add your Social Security Number to the Unique Identity Include List. Social Security Numbers can be used to open credit cards and bank accounts on your behalf, so searching for this Identity Match Type is of critical importance.

By default, Identity Finder will always search for Social Security Numbers using AnyFind. However, you may customize this behavior.

If you are using the Startup Wizard, you can select or deselect the "Social Security Numbers" option and you can choose to add specific, unique Social Security Numbers to the search.

If you are not using the Startup Wizard, you can enable or disable AnyFind searching for Social Security Numbers by clicking the "Social Security" button on the What to Search For ribbon. When the button has an orange highlight, it is enabled and Identity Finder will use AnyFind searching. You can also Add a Social Security Number to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon). Within that dialog box, when Social Security Number is selected in the "Identity Type" drop down box, you can check or uncheck the "Enable Automatic Search for Social Security" to change your AnyFind settings for Social Security Numbers. The ribbon button will update automatically to reflect any changes you make here.

Note: When entering a unique Social Security Number, it must be entered as ###-##-#### with no other characters or spaces. For example "123-12-1234" (without the quotes) is valid. However "123 12 1234" (without the quotes) is invalid because it contains spaces.
What Personal Information to Search For

Passwords

Identity Finder will locate Passwords without requiring you to provide any personal information. It uses the AnyFind proprietary technology to find series of characters that represent Passwords. If you want to always be sure to search for a specific Password, you should add your password to the Unique Identity Include List. If you want to search for only a specific Password, you should disable AnyFind and add your password to the Unique Identity Include List. Passwords can be used to authenticate you online, so searching for this Identity Match Type is of critical importance.

By default, Identity Finder will always search for Passwords using AnyFind. However, you may customize this behavior.

If you are using the Startup Wizard, you can select or deselect the "Passwords" option and you can choose to add specific, unique Passwords to the search.

If you are not using the Startup Wizard, you can enable or disable AnyFind searching for Passwords by clicking the "Password" button on the What to Search For ribbon. When the button has an orange highlight, it is enabled and Identity Finder will use AnyFind searching. You can also Add a Password to the Unique Identity Include List via the Include List page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon). Within that dialog box, when Password is selected in the "Identity Type" drop down box, you can check or uncheck the "Enable Automatic Search for Password" to change your AnyFind settings for Passwords. The ribbon button will update automatically to reflect any changes you make here.

Note: When entering a unique Passwords, it must be between 3 and 25 characters.
Identity Finder will locate Dates of Birth without requiring you to provide any personal information. It uses the AnyFind proprietary technology to find numeric Dates of Birth in multiple formats. If you want to search for only a specific Date of Birth or want to find the written out version (i.e., January 1, 1970 as opposed to 01/01/1970), you should disable AnyFind and add your Date of Birth and use Unique Searching Using Your Personal Information to find your Date of Birth in a variety of additional formats. Dates of Birth are commonly used as a way to authenticate you over the phone as companies typically ask you to confirm you are who you say by stating your Date of Birth, so searching for this Identity Match Type is of high importance.

If you are using the Startup Wizard, you can choose to add specific, unique Dates of Birth to the search.

If you are not using the Startup Wizard, you can also Add a Date of Birth to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon).

You can enable or disable AnyFind searching for Dates of Birth by clicking the "Date of Birth" button on the What to Search For ribbon. When the button has an orange highlight, it is enabled and Identity Finder will use AnyFind searching. You can also Add a Date of Birth to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon). Within that dialog box, when Date of Birth is selected in the "Identity Type" drop down box, you can check or uncheck the "Enable Automatic Search for Dates of Birth" to change your AnyFind settings. The ribbon button will update automatically to reflect any changes you make here.

Note: When entering a unique Date of Birth, it must be entered as mm/dd/yyyy with no other characters or spaces. For example "03/12/1972" (without the quotes) is valid. However "03-12-1972" (without the quotes) is invalid because it contains dashes.
Driver's Licenses

Identity Finder will locate Driver's Licenses if you provide specific personal information. It uses Unique Searching Using Your Personal Information to find your Driver's Licenses. Driver's Licenses are commonly used as a way to identity who you are, so searching for this Identity Match Type is of high importance.

Identity Finder will not search for Driver's Licenses until you provide specific personal information.

If you are using the Startup Wizard, you can choose to add specific, unique Driver's Licenses to the search.

If you are not using the Startup Wizard, you can also Add a Driver's License to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon).

Note: When entering a unique Drivers License, it must be entered as 5-20 letters, numbers, dashes or spaces but without any other characters. For example "WI-123456789" (without the quotes) is valid. However "#123456789" (without the quotes) is invalid because it contains a number sign (#).
**Personal Addresses**

Identity Finder will locate Personal Addresses if you provide specific personal information. It uses [Unique Searching Using Your Personal Information](#) to find your Personal Addresses in a variety of formats. Personal Addresses are commonly used as a way to authenticate you over the phone as companies typically ask you to confirm you are who you say by stating your Personal Address, so searching for this [Identity Match Type](#) is of high importance.

Identity Finder will not search for Personal Addresses until you provide specific personal information.

If you are using the [Startup Wizard](#), you can choose to add specific, unique Personal Addresses to the search.

If you are not using the Startup Wizard, you can also [Add a Personal Address to the Unique Identity Include List](#) via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon).

Note: When entering a unique Personal Address, it must be entered as no more than 100 letters, numbers, dashes, spaces, periods, colons, commas, or slashes (/), but without any other characters. Your address must be entered all on one line and you should separate it with commas rather than new lines just as if you were addressing an envelope.

For example "10 West 10th St., New York, NY, 10011" (without the quotes) is valid. However "10 West 10th St. + New York + NY + 10011" (without the quotes) is invalid because it contains plus signs (+). Additionally "10 West 10th St. New York NY 10011" (without the quotes) is valid, however it is unlikely to match anything because it does not have commas to separate the fields and therefore will only match if the address was written on one line.
Passport Numbers

Identity Finder will locate Passport Numbers if you provide specific personal information. It uses Unique Searching Using Your Personal Information to find your Passport Numbers. Passport Numbers are used as a way to identify who you are, so searching for this Identity Match Type is of high importance.

Identity Finder will not search for Passport Numbers until you provide specific personal information.

If you are using the Startup Wizard, you can choose to add specific, unique Passport Numbers to the search.

If you are not using the Startup Wizard, you can also Add a Passport Number to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon).

Note: When entering a unique Passport Number, it must be entered as 9 digits without any other characters. For example "123456789" (without the quotes) is valid. However "#123456789" (without the quotes) is invalid because it contains a number sign (#).
Identity Finder will locate Telephone Numbers if you provide specific personal information. It uses **Unique Searching Using Your Personal Information** to find your Telephone Numbers in a variety of formats. Telephone Numbers are used as additional information about who you are, so searching for this **Identity Match Type** is of importance.

Identity Finder will not search for Telephone Numbers until you provide specific personal information.

If you are using the **Startup Wizard**, you can choose to add specific, unique Telephone Numbers to the search.

If you are not using the Startup Wizard, you can also **Add a Telephone Number to the Unique Identity Include List** via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon).

**Note:** When entering a unique Telephone Number, it must be entered as ###-###-#### with no other characters or spaces. For example "212-555-1234" (without the quotes) is valid. However "(212) 555-1234" (without the quotes) is invalid because it contains parentheses, dashes, and spaces.
Employee IDs

Identity Finder will locate Employee IDs if you provide specific personal information. It uses Unique Searching Using Your Personal Information to find your Employee IDs. Employee IDs are used as additional information about who you are, so searching for this Identity Match Type is of importance.

Identity Finder will not search for Employee IDs until you provide specific personal information.

If you are using the Startup Wizard, you can choose to add specific, unique Employee IDs to the search.

If you are not using the Startup Wizard, you can also Add an Employee ID to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon).

Note: When entering a unique Drivers License, it must be entered as no more than 25 letters, numbers, dashes or spaces but without any other characters. For example "00400012345" (without the quotes) is valid. However "#00400012345" (without the quotes) is invalid because it contains a number sign (#).
Mother's Maiden Names

Identity Finder will locate Mother’s Maiden Names if you provide specific personal information. It uses Unique Searching Using Your Personal Information to find your Mother’s Maiden Names in a variety of formats. Mother's Maiden Names are commonly used as a way to authenticate you over the phone as companies typically ask you to confirm you are who you say by stating your Mother's Maiden Name, so searching for this Identity Match Type is of high importance.

Identity Finder will not search for Mother's Maiden Names until you provide specific personal information.

If you are using the Startup Wizard, you can choose to add specific, unique Mother's Maiden Names to the search.

If you are not using the Startup Wizard, you can also Add a Mother's Maiden Name to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon).

Note: When entering a unique Mother’s Maiden Name, it must be entered as no more than 50 letters, dashes or spaces but without any other characters. For example "Smith-Jones" (without the quotes) is valid. However "Smith/Jones" (without the quotes) is invalid because it contains a slash (/).
User Defined Types

This feature is only available in Professional and Enterprise Editions.

Identity Finder provides the ability for you to enter your own User Defined Identity Match Type to search for anything else that is not captured by another Identity Match Type. For example a specific personal healthcare record, an account id, or a keyword like "crime". It uses Unique Searching Using Your Personal Information to find your User Defined Types in the specific format you provide.

Identity Finder will not search for User Defined Identity Matches until you provide specific personal information. The information you enter is case sensitive.

If you are using the Startup Wizard, you can choose to add specific, unique User Defined Identity Matches to the search.

If you are not using the Startup Wizard, you can also Add a User Defined Identity Match to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon). With the Enterprise Edition you may use Regular Expressions to define your search criteria. Check the Enable RegEx Search for all User Defined Types to enable this feature.
Note: When entering a unique User Defined Identity Match, it must be entered as no more than 100 characters.
Australia Tax File Number

Identity Finder will locate Australian Tax File Numbers without requiring you to provide any personal information. It uses the AnyFind proprietary technology to find valid Tax File Numbers. If you want to search for only a specific Tax File Number, you should disable AnyFind and add your Tax File Number to the Unique Identity Include List. Tax File Numbers are used in Australia and can be used to open credit cards and bank accounts on your behalf, so searching for this Identity Match Type is of critical importance if you are from Australia.

By default, Identity Finder will not search for Tax File Numbers. However, you may customize this behavior.

If you are using the Startup Wizard, you can choose Yes to AnyFind Worldwide Searching and then select "Tax File Number" option.

If you are not using the Startup Wizard, you can enable or disable AnyFind Worldwide Searching for Tax File Numbers by first clicking the Settings button on the Tools and Options ribbon, then selecting the Worldwide Search page from the left menu. Click the Enable Tax File Number (TFN) Search checkbox. This will alter the appearance of your What to Search for ribbon and add "AU: TFN" to the AnyFind Automatic Search group. It will be also now be enabled and ready for searching. When the button has an orange highlight, it is enabled and Identity Finder will use AnyFind searching. You can also Add a Tax File Number to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon). Within that dialog box, when Tax File Number is selected in the "Identity Type" drop down box, you can check or uncheck the "Enable Automatic Search for Social Security" to change your AnyFind settings for Tax File Numbers. The ribbon button will update automatically to reflect any changes you make here.

Note: You will not see the AU:TFN or Australia Tax File Number options in the AnyFind Automatic Search or Unique Identity Include List unless you have Enabled Worldwide Searching.
Canada Social Insurance Number

Identity Finder will locate Canadian Social Insurance Numbers without requiring you to provide any personal information. It uses the AnyFind proprietary technology to find valid Social Insurance Numbers. If you want to search for only a specific Social Insurance Number, you should disable AnyFind and add your Social Insurance Number to the Unique Identity Include List. Social Insurance Numbers are used in Canada and can be used to open credit cards and bank accounts on your behalf, so searching for this Identity Match Type is of critical importance, if you are from Canada.

By default, Identity Finder will not search for Social Insurance Numbers. However, you may customize this behavior.

If you are using the Startup Wizard, you can choose Yes to AnyFind Worldwide Searching and then select "Social Insurance Number" option.

If you are not using the Startup Wizard, you can enable or disable AnyFind Worldwide Searching for Social Insurance Numbers by first clicking the Settings button on the Tools and Options ribbon, then selecting the Worldwide Search page from the left menu. Click the Enable Social Insurance Number (TFN) Search checkbox. This will alter the appearance of your What to Search for ribbon and add "Canada: SIN" to the AnyFind Automatic Search group. It will be also now be enabled and ready for searching. When the button has an orange highlight, it is enabled and Identity Finder will use AnyFind searching. You can also Add a Social Insurance Number to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon). Within that dialog box, when Social Insurance Number is selected in the "Identity Type" drop down box, you can check or uncheck the "Enable Automatic Search for Social Insurance" to change your AnyFind settings for Social Insurance Numbers. The ribbon button will update automatically to reflect any changes you make here.

Note: You will not see the Canada: SIN or Canada Social Insurance Number options in the AnyFind Automatic Search or Unique Identity Include List unless you have Enabled Worldwide Searching.
United Kingdom National Insurance Number

Identity Finder will locate United Kingdom National Insurance Numbers without requiring you to provide any personal information. It uses the AnyFind proprietary technology to find valid National Insurance Numbers. If you want to search for only a specific National Insurance Number, you should disable AnyFind and add your National Insurance Number to the Unique Identity Include List. National Insurance Numbers are used in the United Kingdom and can be used to open credit cards and bank accounts on your behalf, so searching for this Identity Match Type is of critical importance, if you are from the United Kingdom.

By default, Identity Finder will not search for National Insurance Numbers. However, you may customize this behavior.

If you are using the Startup Wizard, you can choose Yes to AnyFind Worldwide Searching and then select "National Insurance Number" option.

If you are not using the Startup Wizard, you can enable or disable AnyFind Worldwide Searching for National Insurance Numbers by first clicking the Settings button on the Tools and Options ribbon, then selecting the Worldwide Search page from the left menu. Click the Enable National Insurance Number (NINO) Search checkbox. This will alter the appearance of your What to Search for ribbon and add "UK: NINO" to the AnyFind Automatic Search group. It will be also now be enabled and ready for searching. When the button has an orange highlight, it is enabled and Identity Finder will use AnyFind searching. You can also Add a National Insurance Number to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon). Within that dialog box, when National Insurance Number is selected in the "Identity Type" drop down box, you can check or uncheck the "Enable Automatic Search for National Insurance Numbers" to change your AnyFind settings for National Insurance Numbers. The ribbon button will update automatically to reflect any changes you make here.

Note: You will not see the UK: NINO or United Kingdom National Insurance Number options in the AnyFind Automatic Search or Unique Identity Include List unless you have Enabled Worldwide Searching.
United Kingdom National Health Service Number

Identity Finder will locate United Kingdom National Health Service Numbers without requiring you to provide any personal information. It uses the AnyFind proprietary technology to find valid National Health Service Numbers. If you want to search for only a specific National Health Service Number, you should disable AnyFind and add your National Health Service Number to the Unique Identity Include List. National Health Service Numbers are used in the United Kingdom and can be used to open credit cards and bank accounts on your behalf, so searching for this Identity Match Type is of critical importance, if you are from the United Kingdom.

By default, Identity Finder will not search for National Health Service Numbers. However, you may customize this behavior.

If you are using the Startup Wizard, you can choose Yes to AnyFind Worldwide Searching and then select "National Health Service Number" option.

If you are not using the Startup Wizard, you can enable or disable AnyFind Worldwide Searching for National Health Service Numbers by first clicking the Settings button on the Tools and Options ribbon, then selecting the Worldwide Search page from the left menu. Click the Enable National Health Service Number (NHS Number) Search checkbox. This will alter the appearance of your What to Search for ribbon and add "UK: NHS" to the AnyFind Automatic Search group. It will be also now be enabled and ready for searching. When the button has an orange highlight, it is enabled and Identity Finder will use AnyFind searching. You can also Add a National Health Service Number to the Unique Identity Include List via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon). Within that dialog box, when National Health Service Number is selected in the "Identity type" drop down box, you can check or uncheck the "Enable Automatic Search for National Health Service Number" to change your AnyFind settings for National Insurance Numbers. The ribbon button will update automatically to reflect any changes you make here.

Note: You will not see the UK: NINO or United Kingdom National Health Service Number options in the AnyFind Automatic Search or Unique Identity Include List unless you have Enabled Worldwide Searching.
Using AnyFind for Automatic Searching

What is Automatic Searching with AnyFind?

AnyFind is an advanced, proprietary technology that automatically searches your computer for certain Identity Match Types. The algorithms within AnyFind make it possible to find Credit Card Numbers, Bank Account Numbers, Social Security Numbers, Passwords, and Dates of Birth without requiring you to enter any personal information. AnyFind will locate your information but will also locate valid Identity Matches for others' as well to uncover any personal information of your family or coworkers stored insecurely on your computer. In addition, by Enabling Worldwide Searching you can automatically find Australia Tax File Numbers, Canada Social Insurance Numbers, United Kingdom National Insurance Numbers, and United Kingdom National Health Service Numbers.

There are multiple ways to Enable AnyFind searching. You can also customize AnyFind settings in the Professional and Enterprise Editions using the AnyFind Settings Page.
Enabling AnyFind

By default, Identity Finder will always enable AnyFind for **Credit Card Numbers**, **Social Security Numbers**, and **Passwords**. AmyFind is also available for **Bank Account Numbers** and **Dates of Birth** (not available via the Startup Wizard). In addition, by **Enabling Worldwide Searching** you can automatically find **Australia Tax File Numbers**, **Canada Social Insurance Numbers**, **United Kingdom National Insurance Numbers**, and **United Kingdom National Health Service Numbers**.

If you are using the **Startup Wizard**, you can enable or disable AnyFind by checking or unchecking the "Credit Card Numbers (or Debit Card)", "Bank Accounts Numbers", "Social Security Numbers", or "Passwords" options.

If you are not using the Startup Wizard, you can enable or disable **AnyFind** searching by clicking the "Credit Card", "Bank Account", "Social Security", "Password", or "Date of Birth" buttons in the "Search Automatically with AnyFind" group on the "What to Search For" ribbon. When a button has an orange highlight, it is enabled and Identity Finder will use AnyFind searching for that **Identity Match Type**.

Additionally, you can change the AnyFind settings via the "Include List" page of the "Identity Finder Personal Information File" dialog box (you can open this dialog box by pushing the Add/Remove Information button on the What to Search for ribbon). Within that dialog box, when "Credit Card Number", "Bank Account Number",
What Personal Information to Search For

"Social Security Number", "Date of Birth", or "Password" is selected in the "Identity Type" drop down box, you can check or uncheck the "Enable Automatic Search for XXXXXXXXX" to change your AnyFind settings for that Identity Type. The associated ribbon button will update automatically to reflect any changes you make here.

See Also: Enabling Worldwide Searching

See Also: AnyFind Settings Page.
**Using Unique Searching**

**What is Unique Searching?**

Unique Searching allows you to find Identity Matches using the specific personal information you provide. However, Identity Finder doesn’t simply search for the personal information you enter, but rather it converts that information into multiple formats to increase the likelihood of discovering matches. For example, when you enter 03/12/1972 as a Date of Birth, Identity Finder will match all of the following formats (and others) in any location:

- 03/12/1972
- 03/12/72
- 03-12-1972
- 03-12-72
- Mar. 12, 1972
- March 12, 1972

Additionally, Identity Finder will also look for any words you enter in various cases so it is not necessary for Maiden Name to enter Smith, smith, and SMITH. Any one of these will match all three versions.

There are multiple ways to enable Unique Searching.
**Advantages of Unique Searching**

Unique Searching allows you to enhance AnyFind and increase the amount of personal information that Identity Finder can locate. The more personal information uncovered the greater protection you will have against Identity Theft. You can enable Unique Searching for all of the Identity Match Types but, if you want Identity Finder to locate and of the following Identity Match Types, you must enter unique information:

- Credit Card Numbers
- Bank Account Numbers
- Social Security Numbers
- Passwords
- Dates of Birth
- Driver's Licenses
- Personal Addresses
- Passport Numbers
- Telephone Numbers
- Employee IDs
- Mother's Maiden Names
- User Defined Types
- Australia Tax File Numbers
- Canada Social Insurance Numbers
- United Kingdom National Insurance Numbers
- United Kingdom National Health Service Numbers

Most of these types also utilize additional, proprietary algorithms to convert the information that you enter into multiple formats to increase the likelihood of discovering matches. This, in combination with AnyFind, maximizes the effectiveness of Identity Finder's ability to prevent identity theft.
**Finding Personal Information with Unique Searching**

Identity Finder will not enable Unique Searching until you provide specific personal information. You can add information using the Startup Wizard or the "Add/Remove Information" button on the "What to Search for" ribbon. If you are using the Startup Wizard, you can choose to add specific, unique information to the search.

<table>
<thead>
<tr>
<th>Personal Identity Information Entry Fields</th>
<th>Unique Identity Include List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Birth</td>
<td>Type</td>
</tr>
<tr>
<td>Driver's License</td>
<td>Add</td>
</tr>
<tr>
<td>Personal Address</td>
<td></td>
</tr>
<tr>
<td>Passport Number</td>
<td></td>
</tr>
<tr>
<td>Telephone Number</td>
<td></td>
</tr>
<tr>
<td>Employee ID</td>
<td></td>
</tr>
<tr>
<td>Mother's Maiden</td>
<td></td>
</tr>
</tbody>
</table>

If you are not using the Startup Wizard, you can also add personal information to the Include List by clicking the "Add/Remove Information" button on the "What to Search for" ribbon. The "Search with Unique Personal Information You Include" group on the "What to Search For" ribbon allows you to enable and disable Unique Searching for each Identity Type. If you have not provided any personal information for an Identity Match Type, that specific type's button will be disabled on the ribbon. After you click OK, the ribbon button for the identity type(s) you included will be highlighted orange. When these button(s) are highlighted, Identity Finder will search for that identity type. If you do not want Identity Finder to search for that identity type for a specific search, but wish to leave the information in your Unique Identity Include List, then click the button to remove the orange highlight.

![Identity Finder Wizard](image)

Note if you Enabling Worldwide Searching then you can also add unique identities for additional identity match types and you might see additional buttons for Australia Tax File Numbers, Canada Social Insurance Numbers, United Kingdom National Insurance Numbers, and United Kingdom National Health Service Numbers. The
Startup Wizard will not let you add personal information for unique searching, but you can add personal information to the Include List by clicking the "Settings" button on the Main ribbon and clicking the Include Unique Identities tab or by clicking the "Add/Remove Information" button on the "What to Search For" ribbon.
Adding and Removing Unique Identities

To view and manage your Unique Identity Include List (a section of your Personal Information File) and add or remove personal information, click the “Add/Remove Information” button on the "What to Search for" ribbon.

To add a unique identity, select the Identity Match Type from the Add an Identity drop down box. Then enter your personal information in the field to its right. Below this field is an example of the acceptable syntax for this identity. It is important for you to use the correct syntax so that Identity Finder can convert your identity into numerous formats for searching. Once you have entered the appropriate identity information, click the "Add" button and it will appear in the Unique Identity Include List.

To remove an identity or multiple identities, highlight them and click the "Remove" button. The "Remove All" button clears the entire list.

If you make changes and want to Save your list for future sessions, click the "Save" button. Otherwise click OK. You may be prompted to provide a password if you are saving a new list.
If Identity Finder did not automatically load your Personal Information File when it started, you can load it now by clicking the "Load" button. You will be prompted for your password.

After you click OK, the ribbon button for the identity type(s) you included in the "Search with Unique Personal Information You Include" group on the What to Search For tab will be highlighted orange:

When these button(s) are highlighted, Identity Finder will search for that identity type. If you do not want Identity Finder to search for that identity type for a specific search, but wish to leave the information in your Unique Identity Include List, then click the button to remove the orange highlight.

Remember you must Enable Worldwide Searching to be able to add unique identities for Worldwide identity types.
What is the Include List?

The Include List allows you to provide unique personal information about an identity. You can securely save this information across sessions of Identity Finder within your Personal Information File. Identity Finder will always search for the information you provide. Your identities are confidential and sensitive so this Include List is stored encrypted on your hard drive and requires a password to be opened.

To open the list, click the "Add/Remove Information" button on the "What to Search for" ribbon. Here you can view all your Unique Identities. If you make changes and want to Save your list for future sessions, click the "Save" button. Otherwise click OK. You may be prompted to provide a password if you are saving a new list.

To add a unique identity, select the Identity Match Type from the Add an Identity drop down box. Then enter your personal information in the field to its right. Below this field is an example of the acceptable syntax for this identity. It is important for you to use the correct syntax so that Identity Finder can convert your identity into numerous formats for searching. Once you have entered the appropriate identity information, click the "Add" button and it will appear in the Unique Identity Include List.
To remove an identity or multiple identities, highlight them and click the "Remove" button. The "Remove All" button clears the entire list.

Note if you Enabled Worldwide Searching then you can also add unique identities for additional identity match types and you might see additional buttons for Australia Tax File Numbers, Canada Social Insurance Numbers, United Kingdom National Insurance Numbers, and United Kingdom National Health Service Numbers.

All the information you enter will be saved to your Personal Information File (PIF). If you did not load this file on startup or you want to revert your changes to the last time you saved, you may press the "Load PIF" button. If you want your changes saved to your PIF, click the "Save PIF" button.

After you click OK, the ribbon button for the identity type(s) you included in the "Search with Unique Personal Information You Include" group on the What to Search For tab will be highlighted orange. When these button(s) are highlighted, Identity Finder will search for that identity type. If you do not want Identity Finder to search for that identity type for a specific search, but wish to leave the information in your Unique Identity Include List, then click the button to remove the orange highlight.

Note: Only unique identities that you add before a search begins will be found during that search. If you add unique identities to the Include List during a search, they will not be used for the current search.

Note: Identity Finder doesn’t simply search for the personal information you enter, but rather it converts that information into multiple formats to increase the likelihood of discovering matches. For example, when you enter 03/12/1972 as a Date of Birth, Identity Finder will match all of the following formats (and others) in any location:

- 03/12/1972
- 03/12/72
- 03-12-1972
- 03-12-72
- Mar. 12, 1972
- March 12, 1972

Note: Identity Finder will also look for any words you enter in various cases so it is not necessary for Maiden Name to enter Smith, smith, and SMITH. Any one of these will match all three versions.

Note: Choose a strong password to be sure your list is safe.
Where to Search for Personal Information

File Locations

What are File Locations?

File Locations are enabled if you enable searching for Files or Compressed Files. You may select whether you want to search within your My Documents (including User Settings), your My Computer (which includes all of your hard drives), or a Custom folder (or folders) of your choice. Once specified, Identity Finder will search for files (either Common File Types, All Filterable File Types, Custom File Type List, or All Files) and compressed files within that folder and all of its subfolders. Your currently selected option will be highlighted in orange.
Custom Folder List

The Custom button allows you to specify any folder or set of folders to search. When you choose "Custom", the Custom Folder List dialog box will appear. First, you must enter a folder path to search or click the "..." button to browse for one. Second, click the "Add" button and to add the folder to the Custom Folder List box. For each folder you select, all its subfolders will also be searched. You may add as many additional folders as you wish.

If you would like to specify the folder as an exclusion, click the Add as Exclusion checkbox. This will prevent Identity Finder from searching that specific folder and all its subfolders. A common folder to exclude might be c:\windows.

All the information you enter will be automatically saved to your Personal Information File (PIF). If you want to revert your changes to the last time you saved or clicked OK or Apply, you may press the "Load PIF" button. Your changes will be automatically saved when you click OK or Apply.
Where to Search for Personal Information

Custom Folder List [Enterprise]

The Custom button allows you to specify any folder or set of folders to search. When you choose "Custom...", the Custom Folder List dialog box will appear. First, you must enter a folder path to search or click the "..." button to browse for one. Second, click the "Add" button and to add the folder to the Custom Folder List box. For each folder you select, all its subfolders will also be searched. You may add as many additional folders as you wish.

If you would like to specify the folder as an exclusion, click the Add as Exclusion checkbox. This will prevent Identity Finder from searching that specific folder and all its subfolders. A common folder to exclude might be c:\windows.

You can also search for a UNC path using Enterprise Edition so you can enter \1.2.3.4\c$ or map the drive manually and search the drive letter. To search multiple computers, see Searching Multiple Remote Computers for more information.
Where to Search for Personal Information

All the information you enter will be saved to your Personal Information File (PIF). If you did not load this file on startup or you want to revert your changes to the last time you saved, you may press the "Load PIF" button. If you want your changes saved to your PIF, click the "Save PIF" button.
My Documents and Settings Folders

The My Documents and Settings Folders (labeled as My Documents) button specifies that Identity Finder will search the currently logged in user's My Documents and User Settings folders. These folders are typically located at C:\Documents and Settings\USERNAME in Windows XP and C:\Users\USERNAME in Windows Vista however if they are not located in their default location, Identity Finder will automatically detect this and search the correct locations.

If this option is selected, the "My Documents" button on the "Where to Search" ribbon will be highlighted orange.
The My Computer button specifies that Identity Finder will search all drives (removable and local) on your computer, except network drives. If you require the ability to search Network Drives, please purchase the corporate version of Identity Finder available on our website.

If this option is selected, the "My Computer" button on the "Where to Search" ribbon will be highlighted orange.
Searching Multiple Remote Computers Enterprise

This feature is only available in Enterprise Edition.

The Remote button allows you to specify any folder or set of folders to search. When you choose "Remote...", the Remote Computer List dialog box will appear.

First, inside the "Add remote computer names" group, list all your remote machines that you want to search. You may list IP Addresses, NetBIOS Names, or Fully Qualified Domain Names (FQDN). Group them based on how you authenticate because you can specify credentials. List one computer per line (press CTRL-ENTER to go to the next line). You must specify a NetBIOS name, IP Address, or FQDN.

Second, choose whether you want Identity Finder to search all physical drives on the remote machines. If you do not check this box, Identity Finder will still authenticate using the credentials you specified, but you will need to enter the paths you want to search in the Custom Location dialog box. This allows you to search for a UNC path (i.e., \1.2.3.4\c$).
Third, choose whether you want to authenticate with specific credentials or whether you are already authenticated. If you want to specify credentials, click the "Specify authentication credentials" checkbox and enter a username and password. If you do not specify credentials, Identity Finder will try to authenticate using pre-existing credentials on your computer. Either your currently logged in credentials must work, or you must have made a net use connection or to that computer.

All the information you enter will be saved to your **Personal Information File** (PIF). If you did not load this file on startup or you want to revert your changes to the last time you saved, you may press the "Load PIF" button. If you want your changes saved to your PIF, click the "Save PIF" button.

**Note:** After you have selected "Remote..." you will notice that the E-Mails and System groups are disabled. This is because when searching remote computers it is only possible to search their file systems.
Home and Office Files

What are Home and Office Files?

Home and Office Files include all files on your computer that can be read by Identity Finder. Identity Finder can search more than 200 of the most common file types using its built-in filters and a built-in feature of Microsoft Windows available since Windows 2000 called IFilters. For these filterable file types, Identity Finder can search the file while preserving the format and structure of the file. Additionally, Identity Finder can attempt to extract text from any file. As new, proprietary file types are created that Identity Finder cannot search while preserving format and structure, additional IFilters may be created to search them. If you install any of these additional IFilters, Identity Finder will automatically detect and utilize them for all of your future searches. See Installing Additional Filters for more information. To speed your searching, you can enable searching only common file types or searching only filterable file types.

You can enable searching of Files and Compressed Files by clicking their respective buttons. If enabled, the "Files" and/or "Compressed Files" buttons on the "Where to Search" ribbon will be highlighted orange.
Where to Search for Personal Information

Files

You can enable searching of Files by clicking the "Files" button on the "Where to Search" ribbon. When enabled, the button will be highlighted orange. Identity Finder will search for files (except compressed files) in the File Location you specify.

Identity Finder can read over 200 file types while preserving format and structure. If there is a file type that you must search while preserving format and structure and it is not currently supported natively, you may be able to install an additional IFilter. Additionally, Identity Finder can extract readable text from any type of file. To speed your searching, you can enable searching only common file types or searching only filterable file types.

File types searchable by Identity Finder:

- Microsoft OneNote 2003, 2007 (note: requires OneNote or Filter Pack to be installed)
- Plain Text Files (extensive list available upon request)
  - ANSI
  - Unicode
  - Batch Files
  - Source Code Files
  - Cookies
  - Instant Messenger Logs
- Rich Text Format
- Web Pages
- Adobe Acrobat (All versions including 8.x)
- Compressed Zip Files
- Any other file (Microsoft Visio Drawings, Microsoft Project Plans, Image Files, Video Files, Music Files, etc.)
Compressed Files

You can enable searching of Compressed Files by clicking the "Compressed Files" button on the "Where to Search" ribbon. Compressed files are archives that contain additional files. When enabled, the button will be highlighted orange. Identity Finder will search for compressed files in the File Location you specify.
E-Mails

What are E-Mails?

E-Mails include all E-Mail messages on your computer and their attachment files, that can be read by Identity Finder. Identity Finder can read from several E-Mail programs including Outlook, Outlook Express, and Windows Mail. Identity Finder will also automatically search Contacts, Calendar Entries, and Tasks, but you may disable the searching of these items by de-selecting their folders in the E-Mail Settings. If there have a different E-Mail program, you can check to see if an IFilter is available. Note that Identity Finder cannot search E-Mail that is not stored on your computer that you use a web browser to read.

You can enable searching of Messages and Attachments by clicking their respective buttons. If enabled, the "Messages" and/or "Attachments" buttons on the "Where to Search" ribbon will be highlighted orange.
Where to Search for Personal Information

**Messages**

![Identity Finder Interface](image)

You can enable searching of **E-Mail** Messages (including Calendar entries, contacts, and tasks) by clicking the "Messages" button on the "Where to Search" ribbon. When enabled, the button will be highlighted orange. You can also specify if you wish to search inside **attachments**.
Attachments

You can enable searching of Attachments by clicking the "Attachments" button on the "Where to Search" ribbon. When enabled, the button will be highlighted orange. Identity Finder will search inside attachments, if a message contains any. However, by default attachments that contain compressed files will not be searched unless you also select the Compressed Files option.
System Areas

What are System Areas?

System Areas include many of the hidden areas on your computer you might not typically have access to or even realize exist. Identity Finder can read these areas including the Windows Registry and Hidden Web Data for browsers including Microsoft Windows Internet Explorer and Mozilla Firefox.

You can enable searching of Hidden Web Data and the Windows Registry by clicking their respective buttons. If enabled, the "Hidden Web Data" and/or "Windows Registry" buttons on the "Where to Search" ribbon will be highlighted orange.
Hidden Web Data

Searching within Hidden Web Data is a very powerful feature because it will search one of your most commonly used applications for personally identifiable information: your web browser. Your web browser may automatically, and without your knowledge, save your passwords and form data (sometimes referred to as AutoComplete data) when you interact online. This information commonly contains credit card information or a password to a merchant. Identity Finder can uncover this information and secure or shred it. You can enable searching of Hidden Web Data by clicking the "Hidden Web Data" button on the "Where to Search" ribbon. When enabled, the button will be highlighted orange.
Windows Registry

The Windows Registry is where applications typically save their configuration information. Sometimes for registration or convenience purposes personally identifiable information will be saved in the registry. For example, an application may save your password in the registry so you are not required to enter it each time the application opens. Additionally, an application may use the registry to save the personal registration information you provided during its installation process.

Note: Identity Finder never stores any of your personally identifiable information in the Windows Registry.

Identity Finder can find application-stored information and shred it. You can enable searching of the Windows Registry by clicking the "Windows Registry" button on the "Where to Search" ribbon. When enabled, the button will be highlighted orange.
Finding Personal Information

Starting a Search

Customizing Your Search

You can customize your search by choosing options on the What to Search For ribbon and Where to Search ribbon.

What to Search For

- **AnyFind for Automatic Searching**
- **Unique Identity Searching**

Where to Search

- **File Locations**
- **Home and Office Files**
- **E-Mails**
- **System Areas**
Initiating a Search

Once you have customized your search or decided to use the default search settings, you can click the "Start" button on the Main ribbon and Identity Finder will begin searching the locations you selected.

You may interact with the results as they are displayed or you may wait until Identity Finder has completed its search and use the Results Wizard.
Pausing or Stopping a Search

Pausing and Resuming a Search in Progress
You may temporarily pause a search in progress by clicking the "Pause" button on the Main ribbon. The "Pause" button is in the same place as the "Start" button and is automatically changed from "Start" to "Pause" when a search begins. Once you click "Pause", it will be automatically changed into a "Resume" button.

To resume your search, click the "Resume" button, which is in the same place as the "Pause" and "Start" buttons on the Main ribbon.

Pausing a search is 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. In this case however, it might be more helpful to allow other programs to take priority over Identity Finder by enabling the Give Other Programs Priority Over Identity Finder option.
Stopping a Search in Progress

If you want to stop the current search, click the "Stop" button on the Main ribbon. It will not be possible to resume the search once you click "Stop". If you want to be able to resume your search, use the "Pause" button instead.

Once you click "Stop", Identity Finder will take a moment to complete the current process. You will see a dialog box notifying you of its status. If the location currently being analyzed is large or complex, it may take a long time for Identity Finder to stop your search. The hourglass animation will let you know that Identity Finder is work on your request.

After the search has been stopped, if there are results, you will be prompted to initiate either the Results Wizard or advanced mode to begin protecting your personally identifiable information. If there are no results, you will be prompted to initiate a new search or to exit Identity Finder.
Finding Personal Information

Reviewing Results

Using the Previous and Next Buttons

You can use the "Previous Match" and "Next Match" buttons on the Main ribbon to seek to Identity Matches within the result that you are previewing. You may not use these previous and next buttons to seek to another identity match, if it is in a different location. To skip to another location, such as a file or E-Mail message, you can use the arrow keys or your mouse.
Anatomy of the Results View

The results view is a reporting table, similar to a spreadsheet, that is on the left side of Identity Finder. It has a header across the top that contains the following column headers:

<table>
<thead>
<tr>
<th>Column Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checkbox (Selected)</td>
<td>Allows you to select multiple results and perform an action of your choice using the ribbon or right-click menu. To select or deselect all locations, you may left click on this column header.</td>
</tr>
<tr>
<td>Icon (Location Type)</td>
<td>System generated icon to represent the location type. You may hover the mouse cursor over the icon to see a detailed description of the location type.</td>
</tr>
<tr>
<td>Location</td>
<td>Shows the full path to where on your computer the result resides.</td>
</tr>
<tr>
<td>+/- Tree (Group)</td>
<td>Expandable and collapsible tree icon for results that contain multiple unique identity matches. You may click on the +/- to show or hide the unique identity matches for a location.</td>
</tr>
<tr>
<td>Icon (Identity Type)</td>
<td>Identity Finder generated icon that represents the identity match type. You may hover the mouse cursor over the icon to see a detailed description of the identity match type.</td>
</tr>
<tr>
<td>Identity Match</td>
<td>The actual identity match found by Identity Finder. Your actual identity, such as credit card number, will be displayed here. (Note: Passwords may be hidden or masked)</td>
</tr>
<tr>
<td># (Number of Instances of the Match)</td>
<td>For a parent row this shows the total number of identity matches in the location. For child rows, this shows the quantity of that exact identity match found.</td>
</tr>
</tbody>
</table>

You may choose which column headers you want to see in the results pane. Right-click on the column header and choose Columns. Each column header available to you is shown in the submenu. Put a check (by left-clicking) next to each column header you want displayed.
You may sort your results by clicking on specific column headers. You can have a primary, secondary, tertiary (and beyond) sort order by first left-clicking on a specific column header, then while holding SHIFT, left-clicking again on a second column header (or third or fourth, etc.). You may also use the right mouse button context menu and to right-click on the header for the column you want to sort and choose Sort then choose to Sort Ascending or Sort Descending. Right-clicking on additional headers will allow you to edit the existing sort options or enable sorting by secondary, tertiary, etc.

Note: Clicking the Checkbox column header will select or deselect all of your results. It will not sort. To sort this column, you must right-click on the column header and then select your sort preferences.
Expanding and Collapsing Rows

Identity Finder may uncover multiple unique identity matches within a location. Unique identity matches are distinct from multiple occurrences of the same identity match. For example, when five different passwords are discovered in a file there are five unique identity matches, however, when five instances of the same password are discovered in one file there are five occurrences of that specific password.

When Identity Finder uncovers multiple unique identity matches within a single result, a parent row will be displayed in the results view that says "Multiple Matches" with a total counter of all matches in the location. Each unique match will be displayed in a child row beneath the parent. By default, all parent rows are expanded to allow you to see all of the matches uncovered by Identity Finder. You may choose to collapse these row for ease of viewing by clicking the "Collapse All Rows" button on the Main ribbon. When you do this, two things occur: 1. All parent rows are collapsed, not just the row you have highlighted and 2. The button changes to "Expand All Rows" so that you can later expand all of the rows.

To expand or collapse a single parent row, you may click on the +/- icon just to the left of the words "Multiple Matches."

To control how many child rows are displayed when many multiple unique matches exist, see Restrict the Number of Identity Matches Displayed per Location.
Filtering Results

What is Filtering?
Filtering your results allows you to search through the results in your view and temporarily hide any that do not meet your criteria. To turn on filtering, click the "Filter Results" button on the Main ribbon.

To search by keyword(s), begin typing in the "Filter Results For" field and results that do not match your criteria will immediately be hidden. The keyword filter acts on both the Location and Identity Match columns. You may also use the identity type drop down box to select only the identity types you want to see. For example if you wish only to see passwords or social security numbers.

The keyword and identity type filters work together to allow you to further refine your results. If you wish to search only by keyword, ensure that "All Identity Types" is visible in the identity type filter. If you wish to search only by identity type, ensure that the keyword filter is blank.

You may clear or remove your filter at anytime. Note that while the filter is active, the "Filter Results" button will be highlighted orange.
Resetting Your Filter

To reset or clear your filter and view all results, click the "Show All" button on the filter, or click the "Filter Results" button on the Main ribbon. When you click the "Filter Results" button on the Main ribbon, the filter bar will disappear, all filters will be cleared and the "Filter Results" button will no longer be highlighted orange.
Using the Preview Pane

How to Use the Preview Pane

The Preview Pane is enabled by default but can be turned on and off by clicking the "Preview Pane" button on the Main ribbon. The Preview Pane displays an unformatted version of the result you have selected. The header of the Preview Pane is shaded blue and contains information about the result. The main body of the Preview Pane contains the full content where your result was located with all the Identity Matches highlighted in yellow. You can seek through highlighted matches and review the criticality of your result.

From: support@velosecure.com
Subject: Login Info
Date: Sat 1/20/2007 4:23 PM
Identity Type: 1 Password

Dear Alice Smith,

Thank you for signing up for Identity Finder development community! You may login and activate your account by visiting:

http://www.identityfinder.com/
Login: alicsmith
Password: MyPassword03

Thank you for your business and we look forward to working with you!

Best regards,

Velosecure Support Team
velosecure, LLC
support@velosecure.com
http://www.velosecure.com
http://www.identityfinder.com
Seeking Through Highlighted Matches

When using the Preview Pane you can use the “Previous Match” and “Next Match” buttons on the Main ribbon to seek to Identity Matches within the result that you are previewing. You may not use these previous and next buttons to seek to another identity match if it is in a different location. To skip to the next location, such as a file or E-Mail message, you can use the arrow keys or your mouse.

Each Identity Match will be highlighted in yellow and the current match you are reviewing will be positioned near the top of the Preview Pane. As you use these previous and next buttons to seek through highlighted matches, you might see the Preview Pane jump around as the identity matches do not necessarily appear sequentially in the location.
Working with the Status Window

Anatomy of the Status Window

The Status Window provides a real-time summary of your current search and is composed of the Current Status, Total Locations Searched, and Total Identity Matches groups as well as the Hide and More/Less button. To view the status window, click the "Status Window" button on the Main ribbon.

Current Status
This group box contains the name of the location currently being searched as well as two Progress Bars. Sometimes a notification message will be displayed in the Searching field, such as "Opening Mailboxes". There are two progress bars: Current Progress and Total Progress. The Current Progress Bar depicts this percentage complete for the current Area. The Total Progress is made up of a number of Areas. Locations might have one or more Areas. For example, Hidden Web Data is a location, but searching Internet Explorer Passwords is one Area and Firefox Passwords is another area. To the right of Total Progress is Current Area / Total Areas. While Identity Finder is working, the magnifying glass will be animated to the left of the word Searching. This group also contains subtotals of the following items:

- Total Locations Searched - This is the total number of items of all types searched on your computer so far.
- Locations Searched with Matches - This is the total number of the Items Searched so far that contain at least one Identity Match.
- Total Identity Matches - This is the total number of Identity Matches found so far across all locations.

Total Locations Searched
This group box shows a detailed view of all the identity locations searched so far and the specific number of each type. The total of all the counters in this group equals the Total Location Searched counter in the Summary group.

Total Identity Matches
Finding Personal Information

This group box shows a detailed view of all the identity match types found so far and the specific number of each type. The total of all the counters in this group equals the Total Identity Matches counter in the Summary group.

Buttons

There are two buttons, Hide and Less. Hide will remove the Status Window from your view. To bring it back, click the "Status Window" button on the Main ribbon. Less will compact the Status Window and change to More.
Hiding and Compacting the Status Window

Showing and Hiding
The Status Window is enabled by default but can be turned on and off by clicking the "Status Window" button on the Main ribbon. You can also hide the Status Window by clicking the "Hide" button in the Status Window itself.

Compacting and Expanding
The Status Window is expanded by default allowing you to see progress and summary results. If you want to see only the progress, you can click the "Less" button in the Status Window. If you want to restore the full window, click the "More" button at any time.
The Status Window's Progress Bar displays an approximation of the percentage completion level of the current Area being searched. This is only an estimate based on total number of items that Identity Finder must search. While Identity Finder is determining the total amount of locations to search, the status bar will display a set of blocks moving from right to left and back again.

Above the Progress Bar is a display of the current location Identity Finder is searching. If you only want to see the progress bar, click the "Less" button within the Status Window.
Masking (Hiding) Passwords

Hiding Matches from Result View

You can mask your passwords or other Identity Types with asterisks, thereby hiding them from the results view by clicking the "Mask Passwords" button on the Main ribbon. This button will also be renamed automatically to "Mask Matches" when you choose to mask more than just passwords. To configure which Identity Types will be masked, see the Mask Identity Matches help page.

There are several reasons you might want to do this, but you should note it only affects the results view and not the Preview Pane. If you choose to Save your results, the actual passwords will be written to the file, not the asterisks.

Note: If you are highlighted on a result with a masked Identity Match then the actual information, not the asterisks, will be displayed in the Preview Pane highlighted in yellow.
Advantages of Masking Passwords

Masking Passwords (hiding) can be very helpful if you are reviewing your results in a public area such as your workplace or on your laptop in an airport or coffee shop. You might not be aware of how many passwords are actually stored on your computer so if you want to prevent passwords from being displayed, click the "Mask Passwords" button on the Main ribbon.
Saving, Opening, and Printing Results

Saving Results

Depending on your edition, Identity Finder allows you to save the results of your searches in three ways: Identity Finder (*.idf file), Summary Report (*.html file) and Full Export (*.csv file).

- **Identity Finder [All Editions]**: Generates a *.idf file, which is encrypted with a password of your choice and cannot be read by anyone else. Files saved in this format can only be opened from within Identity Finder and allow you to work with your results at any time in the future. This format is useful when you have run a search but wish to take action on your results at a later time. All results are saved and secured using this format.

- **Web Page Report [Professional and Enterprise Editions]**: Generates a report as a *.html file, which contains an analysis of your results including summary information and totals for the number and types of identity matches that were found as well as the locations containing those matches. This report can be used to show trends if you compare it to previous reports. The Web Page Report is not secured and potentially contains location and identity information so you must be careful to protect it. After you are finished with a file in this format, you should use the Identity Finder tools to shred it.

- **Text Export [Enterprise Edition Only]**: Generates a Comma Separated Values (*.csv) file, which is saved unencrypted, in clear text and can be read by anyone with access to your computer. Files saved in this format can be opened in any text editor or spreadsheet program such as Microsoft Excel but cannot be loaded back into Identity Finder. This format is useful when you wish to perform advanced searching, sorting, and reporting of your data in another application. After you are finished with a file in this format, you should use the Identity Finder tools to shred it.

To save your results, click the save icon in the Quick Access menu or in the Application menu. The default save type is Identity Finder Format, a more secure format that you can use to work with your results at any point in the future. When you are ready to work with your saved results, you will need to load your file back into Identity Finder.
Once you choose Save As, the Save As dialog box will open. You may select the folder location and filename for your results. You will see the Options button on the bottom right of this dialog. This allows you to choose what to include in your saved file and allows you to omit information depending on what type of file you are saving.

Once you click the Options button, you will be presented with various choices depending on the save file type:

**Web Page Report:**
Finding Personal Information

Text Export:
Options:

Available in Identity Finder, Web Page Report, and Text Export:
- Save selected (checked) rows only: Allows you to save only the rows you checked from your results. When saving only selected row, the summary information for the entire search is not included in the saved file.

Available in Web Page Report and Text Export only:
- Save selected items: Allows you to save the information from only the that columns you check. You may also choose to redact Identity Matches or all but the last four characters. This is helpful for sending reports from an administrator to system owner for review.
- Save parent rows only: Allows you to save only the parent row from each result. This excludes child rows, those that do not contain a location, as they only contain additional details for the matches in a location.

Available in Text Export only:
- Save Parent/Child rows or Repeat all information on every row: Since this will be read as a matrix it allows you to repeat all information on every row so there are no gaps when printing child rows. Additionally, the Show Multiple Matches row let’s you suppress or display the parent row summary.

Available in Web Page Report only:
- Executive Summary or Save Summary Information: This allows you to save only your summary information that includes the total number of matches found, how many locations were searched, and a breakdown into each category type.
Note: Choose a strong password to be sure your document is safe.
Identity Finder allows you to open the results of your previously saved search, if it was saved as an Identity Finder (*.idf) file. To open your results, click the Open icon in the Quick Access menu or in the Application menu. A browse dialog box will appear allowing you to navigate to your file. Once you select your file, you will be prompted for the password you chose when saving the file. The password is necessary to protect the sensitive information contained within the file. If you have forgotten your password, you will be unable to load your saved results.

Note: Choose a strong password to be sure your document is safe.

Identity Finder also provide you quick access to your most recently saved and loaded Identity Finder files. To load any one of your recent results, simply click on its name in the Recent Results column of the Application menu:
Identity Finder allows you to print the results of your searches as a report for reviewing later. It is important to note that your results are printed in clear text and can be read by anyone who has access to your print out. Please be sure to only print to a printer in a secure location, store the report in a safe place when you are using it, and physically shred it when you are finished.

To print your results, click the print icon in the Application menu.
Protecting Personal Information

Reminder for Taking Actions on Your Identity Matches

When Identity Finder completes its search, you are presented with three options:

- Use the Wizard
- Use Advanced Mode
- Remind Me Later

If you choose to be reminded later, you are presented with several time options. Identity Finder will minimize itself to your system tray and remain there until the specified period of time has passed. If you want to bring Identity Finder back sooner, you can double click the system tray icon.
Securing Identity Matches

Securing Identity Matches: Overview

When Identity Finder locates an Identity Match in any of the following location types, you will be able use the Secure feature to protect your identity:

- Microsoft Office Files
- Securing Microsoft Access Database Files [Professional/Enterprise]
- Compressed Files
- Adobe Acrobat PDF Files
- Text Based and Other Files (Encrypt)
- Text Based Files (Redact) [Professional/Enterprise]
- Microsoft Outlook
- Firefox Hidden Web Data
- Windows Internet Explorer Hidden Web Data
Securing Microsoft Office Files with Encryption

When a Microsoft Office file (Word, Excel, or PowerPoint) has sensitive identity match information in it and you wish to keep the file on your computer, you should utilize the Secure feature to automate the securing of the file with encryption. Depending on the version of Office you have installed, you may be presented with different encryption options.

There are two ways to secure a single Microsoft Office file:
1. Single click the file result with the left mouse button to highlight it and click the "Secure" button on the Main ribbon.
2. Single click the file result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Secure."

To secure multiple office files at one time, check the checkbox of each file and then choose one of the methods described above to begin securing the files. After clicking Secure, a dialog box will open with your available options.

Select the encryption level you want, enter a password to secure the file(s), and click OK. If you click Cancel, no files will be secured. If you click OK and multiple files were selected via their checkboxes, the password and encryption option you provided will be applied to each file. After clicking OK, Identity Finder will secure each file and remove its result row from the Results View allowing you to continue dealing with other, insecure identity matches.
You are also given the option to "Securely store this password in your Password Vault". If you do, the location and password will be saved securely within the Password Vault for you to reference later. Only you have access to your Password Vault because it is only accessible if you authenticate to Identity Finder and load your Personal Information File.

Next time you try to open the file in Microsoft Office, the associated application will prompt you for the password you entered via Identity Finder. If you forget your password, you will not be able to open your file.

Note: Choose a strong password to be sure your document is safe.
Securing Compressed Files

When a compressed file has sensitive identity match information in it and you wish to keep the file on your computer, you should utilize the Secure feature to automate the securing of the file with encryption. Depending on the software you use for uncompressing files, you should be careful to choose the correct encryption options.

There are two ways to secure a single compressed file:

1. Single click the file result with the left mouse button to highlight it and click the "Secure" button on the Main ribbon.
2. Single click the file result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Secure."

To secure multiple compressed files at one time, check the checkbox of each file and then choose one of the methods described above to begin securing the files.
After clicking Secure, a dialog box will open with three available options: Portable, Strong, and Stronger. Select the encryption level you want, enter a password to secure the file(s), and click OK. If you click Cancel, no files will be secured. If you click OK and multiple files were selected via their checkboxes, the password and encryption option you provided will be applied to each file. After clicking OK, Identity Finder will secure each file and remove its result row from the Results View allowing you to continue dealing with other, insecure identity matches.

You are also given the option to "Securely store this password in your Password Vault". If you do, the location and password will be saved securely within the Password Vault for you to reference later. Only you have access to your Password Vault because it is only accessible if you authenticate to Identity Finder and load your Personal Information File.

Next time you try to open the file in your uncompressing application (i.e., Windows or WinZip), the associated application will prompt you for the password you entered via Identity Finder. If you forget your password, you will not be able to open your file.

Note: Portable is the only option available by default within Windows 2000/XP and higher. However it is not a strong encryption option. Strong and Stronger are better options, but will require the use of the Identity Finder Open Secure Zip File Tool or a third party application like Winzip. Strong utilizes 128bit AES encryption and Stronger utilizes 256bit AES encryption.

Note: Choose a strong password to be sure your document is safe.
Securing Adobe Acrobat PDF Files

When an Adobe Acrobat PDF file has sensitive identity match information in it and you wish to keep the file on your computer, you should utilize the Secure feature to automate the securing of the with encryption. Depending on the version of Adobe Acrobat you use, you should be careful to choose the correct encryption options.

There are two ways to secure a single Adobe Acrobat PDF file:

1. Single click the file result with the left mouse button to highlight it and click the "Secure" button on the Main ribbon.
2. Single click the file result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Secure."

To secure multiple Adobe Acrobat PDF files at one time, check the checkbox of each file and then choose one of the methods described above to begin securing the files. After clicking Secure, a dialog box will open with your available options.
Select the encryption level you want, enter a password to secure the file(s), and click OK. If you click Cancel, no files will be secured. If you click OK and multiple files were selected via their checkboxes, the password and encryption option you provided will be applied to each file. After clicking OK, Identity Finder will secure each file and remove its result row from the Results View allowing you to continue dealing with other, insecure identity matches.

You are also given the option to "Securely store this password in your Password Vault". If you do, the location and password will be saved securely within the Password Vault for you to reference later. Only you have access to your Password Vault because it is only accessible if you authenticate to Identity Finder and load your Personal Information File.

Next time you try to open the file in Adobe Acrobat, it will prompt you for the password you entered via Identity Finder. If you forget your password, you will not be able to open your file.

Note: The Low encryption option utilizes 40bit encryption, which is compatible with Adobe Acrobat 3.0 and later. The High encryption option utilizes 128bit encryption, which requires Adobe Acrobat 5.0 and later.

Note: Choose a strong password to be sure your document is safe..
Securing Text Based and Other Files Inside Zip (Encrypt)

When a text based file (i.e., .txt, .html, other files) has sensitive identity match information in it and you wish to keep the file on your computer, you should utilize the Secure feature to automate the securing of this file within an encrypted compressed file. Depending on the software you use for uncompressing files, you should be careful to choose the correct encryption options.

There are two ways to secure a single text based file within an encrypted compressed file:

1. Single click the file result with the left mouse button to highlight it and click the "Secure" button on the Main ribbon.
2. Single click the file result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Secure."

To secure multiple text based files at one time, check the checkbox of each file and then choose one of the methods described above to begin securing the files.
After clicking Secure, a dialog box will open with three available options: Portable, Strong, and Stronger. Select the encryption level you want, enter a password to secure the file(s), and click OK. If you click Cancel, no files will be secured. If you click OK and multiple files were selected via their checkboxes, the password and encryption option you provided will be applied to each file. After clicking OK, Identity Finder will secure each file and remove its result row from the Results View allowing you to continue dealing with other, insecure identity matches.

Each file you choose to secure inside an encrypted compressed zip will named according to its original filename plus a .zip extension at the end. For example, if you secure c:\data files\mydata.txt, you will end up with c:\data files\mydata.txt.zip. Contained inside this encrypted zip will be your original file with no changes. Because your original file contained sensitive identity match information, it will automatically be shredded.

You are also given the option to "Securely store this password in your Password Vault". If you do, the location and password will be saved securely within the Password Vault for you to reference later. Only you have access to your Password Vault because it is only accessible if you authenticate to Identity Finder and load your Personal Information File.

Next time you try to open the file in your uncompressing application (i.e., Windows or WinZip), the associated application will prompt you for the password you entered via Identity Finder. If you forget your password, you will not be able to open your file.
Note: Portable is the only option available by default within Windows 2000/XP and higher. However it is not a strong encryption option. Strong and Stronger are better options, but will require the use of the Identity Finder Open Secure Zip File Tool or a third party application like Winzip. Strong utilizes 128bit AES encryption and Stronger utilizes 256bit AES encryption.

Note: Choose a strong password to be sure your document is safe.
Securing Microsoft Outlook with Password

When Microsoft Outlook has E-Mail messages containing sensitive identity match information and you wish to keep those E-Mail messages on your computer, you should utilize the Secure feature.

Note: Outlook offers a password, which is not very secure, but can prevent inadvertent intrusion by other people who you trust and share your computer with, such as your family at home. For greater security, you should use the "Shred" feature to remove any E-Mail messages that contain sensitive identity match information.

There are two ways to add a password to Microsoft Outlook:

1. Single click any Microsoft Outlook E-Mail message result with the left mouse button to highlight it and click the "Secure" button on the Main ribbon.
2. Single click any Microsoft Outlook E-Mail message result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Secure."

After clicking Secure, a dialog box will open prompting you for a password:

Enter a password and click OK. If you click Cancel, a password will not be applied to Microsoft Outlook. After clicking OK, Identity Finder will apply the password. Because this method does not provide good security, Identity Finder will not remove any Microsoft Outlook E-Mail messages from the Results View.
Protecting Personal Information

You are also given the option to "Securely store this password in your Password Vault". If you do, the location and password will be saved securely within the Password Vault for you to reference later. Only you have access to your Password Vault because it is only accessible if you authenticate to Identity Finder and load your Personal Information File.

Next time you open Microsoft Outlook, it will prompt you for the password you entered via Identity Finder before letting you view your e-mail. If you forget your password, you will not be able to view your E-Mail.

Note: Choose a strong password to be sure your document is safe.
Securing Firefox with a Master Password

When Firefox has saved sensitive passwords and you wish to keep them saved on your computer, you should utilize the Secure feature for Mozilla Firefox Saved Passwords.

When Firefox has saved sensitive form data and you wish prevent it from doing so in the future, you should utilize the Secure feature for Saved Forms (AutoComplete). Firefox Saved Form data cannot be stored securely on your computer.

**Saved Passwords**

You can secure Firefox Saved Passwords with a Master Password that encrypts your entire password database. If you do this, all saved passwords will be secured.

There are three ways to secure all Firefox saved passwords:

1. Single click any Firefox password result with the left mouse button to highlight it and click the "Secure" button on the Main ribbon.
2. Single click any Firefox password result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Secure."
3. Click the Tools and Options ribbon tab and then click the "Secure Firefox" button.

After clicking Secure, a dialog box will open prompting you for a password. Enter a password and click OK. If you click Cancel, no passwords will be secured. After clicking OK, Identity Finder will apply the Master Password and remove all Firefox Saved Password result rows from the Results View allowing you to continue dealing with other, insecure identity matches.
Next time you open Firefox, it will prompt you for the password you entered via Identity Finder before letting you use Saved Passwords. If you forget your password, you will not be able to use Saved Passwords.

You are also given the option to "Securely store this password in your Password Vault". If you do, the location and password will be saved securely within the Password Vault for you to reference later. Only you have access to your Password Vault because it is only accessible if you authenticate to Identity Finder and load your Personal Information File.

Note: Choose a strong password to be sure your data is safe.

**Saved Forms**

Firefox Saved Form data cannot be stored securely on your computer.

There are three ways to prevent Firefox from storing Saved Form data in the future:

1. Single click any Firefox Saved Form data result with the left mouse button to highlight it and click the "Secure" button on the Main ribbon.
2. Single click any Firefox Saved Form data result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Secure."
3. Click the Tools and Options ribbon tab and then click the "Secure Firefox" button.

After clicking Secure, a dialog box will open with the current Firefox setting for Saved Forms. Disable (uncheck) the ability to save form data to secure Firefox.

Next time you use Firefox, it will not save form data for future use. For example, when you are visiting a merchant’s website and enter your personal information to make a purchase, Firefox will not save this information. The downside to this is you will need to retype your personal information every time you visit that site, but this is outweighed by the knowledge that no one can access your personal information via Firefox.
Securing Microsoft Internet Explorer (IE)

When Internet Explorer has saved sensitive passwords and form data and you wish prevent it from doing so in the future, you should utilize the Secure feature. Internet Explorer AutoComplete data cannot be stored securely on your computer.

There are three ways to prevent Internet Explorer from storing AutoComplete data in the future:

1. Single click any Internet Explorer AutoComplete data result with the left mouse button to highlight it and click the "Secure" button on the Main ribbon.
2. Single click any Internet Explorer AutoComplete data result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Secure."
3. Click the Tools and Options ribbon tab and then click the "Secure Microsoft IE" button.

After clicking Secure, a dialog box will open with the current Internet Explorer settings for AutoComplete. Disable (uncheck) the ability to save (1) forms and (2) username and passwords.

Next time you use Internet Explorer, it will not save form data for future use. For example, when you are visiting a merchant’s website and enter your personal information to make a purchase, Internet Explorer will not save this information. The downside to this is you will need to retype your personal information every time you visit that site, but this is outweighed by the knowledge that no one can access your personal information via Internet Explorer.
Shredding Identity Matches

Using Permanent Shredding Feature

When a location has sensitive identity match information in it and you wish to remove it from your computer, you should utilize the Shred feature.

The Shred button is located on the Main ribbon and is enabled for all types of result; however, depending on the location of the result, Shred behaves differently. For files, shred utilizes a secure United States Department of Defense wiping standard known as DOD 5220.22-M. For other locations, shred removes the information from your computer using other, appropriate methods.

There are three ways to Shred a location:
1. Single click the result with the left mouse button to highlight it and click the "Shred" button on the Main ribbon.
2. Single click the result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Shred."
3. Highlight the result by single clicking with the left mouse button or by using the arrow keys and then press the "Delete" key on your keyboard.

Note: It is not possible to "undo" a Shred. Shredded results cannot be recovered. Once you shred something, it is gone.

If you are shredding a Hidden Web Data item, you will be given the option to also add the password to your Password Vault.

If you choose "Shred and Securely Add to Password Vault", the location and password will be saved securely within the Password Vault for you to reference later. Only you have access to your Password Vault because it is
only accessible if you authenticate to Identity Finder and load your Personal Information File. If you choose "Shred but Do Not Add to Password Vault", the password will be shredded and not added to your vault.
Advantages of Shredding

Shred is effective at protecting your identity because it is permanent. While this means you can never get your data back, it also means a hacker or malicious intruder also cannot get your data back. For files, shred utilizes a very secure United States Department of Defense wiping standard known as DOD 5220.22-M. For other locations, shred removes the information from your computer’s hard drive or memory using other, appropriate methods.

What is DOD 5220.22-M?

This is the United States Department of Defense Directive 5220.22-M, which provides baseline standards for the protection of classified information. It uses multiple levels of deletion so that the file you delete may not be recovered, even by undelete programs. You can read more on the Defense Technical Information Center website: [http://www.dtic.mil/whs/directives/corres/html/522022m.htm](http://www.dtic.mil/whs/directives/corres/html/522022m.htm)
Recycling Identity Matches

Using Windows Recycle to Delete Files
If a file does not have sensitive identity match information in it, but you no longer have a use for the file, you may wish to Recycle it.

The Recycle action is available only for files. When other types of locations are selected, the "Recycle" button will be disabled. Before using Recycle for dealing with files with identity matches, please read the Disadvantages to Recycle.

There are two ways to recycle a file using Windows, both of which will move your file into the Recycle Bin:

1. Single click the file result with the left mouse button to highlight it and click the "Recycle" button on the Main ribbon.
2. Single click the file result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Recycle."

It is important to note that the Recycle action uses the Windows Recycle Bin. If you have disabled the Windows Recycle Bin, the Recycle action will cause files to be immediately deleted rather than recycled. This method is still not as secure as using Shred and it is recommended that files containing personally identifiable information be Shredded, not simply deleted or recycled. For more information on enabling or disabling the Windows Recycle Bin, please refer to the Windows help for your specific operating system version.
Disadvantages to Recycle

The Recycle Bin only moves a file from its original location to a hidden recycle folder on your hard drive. The file is not actually deleted. Even after you empty the Recycle Bin, **remnants of your file still exist on your hard drive** and may be in a readable and recoverable form for a long time - thereby allowing anyone who has access to your computer to steal your identity information. Therefore, it is important to use the Shred button to truly eliminate a file. Shred utilizes a secure United States Department of Defense wiping technique to delete files.
Quarantining Identity Matches

Quarantining Files with Identity Matches

The Quarantining Files feature is only available in Enterprise Edition.

![Image of Identity Finder interface]

When a file has sensitive identity match information in it and you wish to securely move the file to another location, you should utilize the Quarantine feature.

Quarantine will move your file and then shred the original so that it cannot be recovered by anyone who gains access to your computer. It is important that you quarantine files to a location that is highly secure, such as an encrypted drive or a storage device to which unauthorized individuals do not have access.

There are two ways to quarantine a single file:

1. Single click the file result with the left mouse button to highlight it and click the "Quarantine" button on the Main ribbon.
2. Single click the file result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Quarantine."

To quarantine multiple files at one time, check the checkbox of each file and then choose one of the methods described above to begin quarantining the files. After clicking Quarantine, a dialog box will open with your available options.

Files may be moved to a default location, which can be specified in Settings, or to an Other location that you can set within the dialog box.
You may also choose to Leave Behind Warning Text Document in Place of File. If you do, a text file will be created in its place named exactly the same as the original file including its extension but with a .txt appended to the end. If your file was c:\test.doc then a file c:\test.doc.txt will be left in its place after it is quarantined. You may also change this setting and the default setting on the Security Settings Page for Quarantine.
Opening Identity Matches

How to Open Results in Associated Application

You may want to view or edit an item in its associated application. For example, if a social security number was found in a document, you may wish to launch Microsoft Word to review the file before taking further action.

You may open a result in its associated Windows application in any of the following four ways:

1. Double-click the result with your left mouse button.
2. Single click the result with the left mouse button to highlight it and click the "Open" button on the Main ribbon.
3. Single click the result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Open."
4. Highlight the result by single clicking with the left mouse button or by using the arrow keys and then press the "Enter" key on your keyboard.

If the result was found inside a file, you can open the folder that contains that file in an explorer window. To perform this action, single click the result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on "Open Folder Location."
Working with Results in Associated Application

After you open a result in its associated application, you may want to either redact (specifically delete) your identity information or save the item with security enabled, such as encryption. All applications work differently so if you do not know how to enable security from within the application, try to secure it using Identity Finder.
Protecting Personal Information

Ignoring Identity Matches and Locations

What is the Ignore List?
The Ignore List contains a list of Locations on your computer and Identity Matches that you have instructed Identity Finder not to search for anymore. This is similar to an approved exceptions list because Identity Finder will never report results if they are in your ignore list. You can securely save this information across sessions of Identity Finder within your Personal Information File.

Identity Finder may uncover a sample credit card number inside a temporary internet file or a public password you do not want to secure. When this happens you can tell Identity Finder to ignore those matches for the current and future searches. Ignored matches are added to an approved exception list so you never see them again.

To manage your Ignore List and add or remove items, click the "Add/Remove Information" button on the What to Search for ribbon and click on the Ignore Identities and Locations tab. Alternatively you can click the "Ignore" button on the Main ribbon and then select the Manage 'Ignore List' option.

Here you can view all your Ignored Identities and Locations. If you make changes and want to Save your list for future sessions, click the "Save" button. Otherwise click OK. You may be prompted to provide a password if you are saving a new list. You can also load an Identity and Location Ignore List at any time by clicking the "Load" button.
All the information you enter will be saved to your Personal Information File (PIF). If you did not load this file on startup or you want to revert your changes to the last time you saved, you may press the "Load PIF" button. If you want your changes saved to your PIF, click the "Save PIF" button.

Note: Choose a strong password to be sure your list is safe.
Ignoring Results

When Identity Finder locates and identity match that you do not care about, you may wish to use the Ignore This Identity Match feature to prevent that information from being displayed in the future.

For example, Identity Finder may uncover a sample credit card number inside a temporary internet file or a public password you do not want to secure. In this case, you can tell Identity Finder to ignore those matches for the current and future searches. Ignored matches are added to an approved exception list, the Identity and Location Ignore List, so you never see them again.

There are three ways to ignore an identity match:

1. Single click the identity match result with the left mouse button to highlight it and click the "Ignore" button on the Main ribbon, then highlight and left-click on "This Identity Match."
2. Single click the identity match result with the right mouse button to highlight it and bring up a context menu, then highlight "Ignore" then highlight and left-click on "This Identity Match."
3. Manually add the identity match to the Ignore List from within the Settings dialog box.

Because ignored identity matches may contain sensitive information, the list is stored in a secured data file, encrypted with a password of your choice. When you save the list for the first time, you will be prompted to provide this password. If you have selected the "Load Unique Identity Match Data on Startup" option, you will be prompted for this password each time you run Identity Finder. If you have selected the "Save Unique Identity Match Data on Exit" option, the password will be used to save your information each time you exit Identity Finder.

Note: Identity Matches that you add to the Ignore List during a search will be ignored for the remainder of the current search.

Note: You can always add or remove identity matches to your Ignore List by Managing Your Identity and Location Ignore List via the "Add/Remove Information" button on the What to Search for ribbon.
Ignoring an Identity Match

There are three ways to view or manage your Ignore Identities and Locations List and add or remove identity matches:

1. Click the "Add/Remove Information" button on the What to Search for ribbon and click on the Ignore Identities and Locations tab.
2. Click the "Ignore" button on the Main ribbon, then highlight and left-click on "Manage 'Ignore List'."
3. Single click on any result with the right mouse button to highlight it and bring up a context menu, then highlight "Ignore" then highlight and left-click on "Manage 'Ignore List'."

To add a unique identity to ignore, select the Identity Match Type from the Ignore an Identity drop down box. Then enter your personal information in the field to its right. It is important for you to enter the information exactly as you wish Identity Finder to ignore it. Unlike the Unique Identity Include List, Identity Finder will not convert your ignore items into various formats. Once you have entered the appropriate identity information, click the "Add" button and it will appear in the Identity and Location ignore List.

To remove an identity or multiple identities, highlight them and click the "Remove" button. The "Remove All" button clears the entire list.

If you make changes and want to Save your list for future sessions, click the "Save" button. Otherwise click OK. You may be prompted to provide a password if you are saving a new list.

If Identity Finder did not automatically load your Personal Information File when it started, you can load it now by clicking the "Load" button. You will be prompted for your password.

Note: Identity Matches that you add to the Ignore List during a search will be ignored for the remainder of the current search.
Ignoring Locations on Your Computer

When Identity Finder finds matches in a location that you do not care about, you may wish to use the Ignore This Location feature to prevent that location from being searched in the future. For example, there may be a website for which you use a public login or a specific file you don't want to search. When this happens, you can tell Identity Finder to ignore those locations for the current and future searches. Ignored locations are added to an approved exception list, the Identity and Location Ignore List, so you never see them again.

There are three ways to ignore a location:

1. Single click the result with the left mouse button to highlight it and click the "Ignore" button on the Main ribbon, then highlight and left-click on "This Location."
2. Single click the result with the right mouse button to highlight it and bring up a context menu, then highlight "Ignore" then highlight and left-click on "This Location."
3. Manually add the Location to the Ignore List from within the Settings dialog box.

Because ignored location may specify a place with sensitive information, the list is stored in a secured, encrypted data file with a password of your choice. When you save the list for the first time, you will be prompted to provide this password. If you have selected the "Load Unique Identity Match Data on Startup" option, you will be prompted for this password each time you run Identity Finder. If you have selected the "Save Unique Identity Match Data on Exit" option, the password will be used to save your information each time you exit Identity Finder.

Note: Locations that you add to the Ignore List during a search will be ignored for the remainder of the current search.

Note: You can always add or remove locations to your Ignore List by Managing Your Identity and Location Ignore List via the "Add/Remove Information" button on the What to Search for ribbon.
Ignoring a Location

To manage your Ignore Identities and Locations List and add or remove file locations, click the Ignore button on the Main ribbon and select "Manage Ignore List" (alternatively, you may click the "Add/Remove Information" button on the What to Search for ribbon and then click on the Ignore Identities and Locations tab). To add a file location to ignore, select the Ignore a File option and click the File Selection button. This button will open a dialog box that allows you to select any file on your computer. After navigating to your desired location, click the "Open" button and the full path to your selected file will be displayed. Once you have selected a file location to ignore, click the "Add" button and it will appear in the Identity and Location Ignore List.

To remove a location or multiple locations, highlight them and click the "Remove" button. The "Remove All" button clears the entire list.

If you make changes and want to Save your list for future sessions, click the "Save" button. Otherwise click OK. You may be prompted to provide a password if you are saving a new list.

If Identity Finder did not automatically Load your Ignore Identities and Locations List when it started, you can load it now by clicking the "Load" button. You will be prompted for your password.

Note: Locations that you add to the Ignore List during a search will be ignored for the remainder of the current search.
Advanced Settings to Customize Your Experience

What are Identity Finder Settings?

Settings within Identity Finder can be configured by choosing the Settings button on the Tools and Options ribbon. Most settings that you modify are saved to your computer and remembered by Identity Finder when you start the application. You can configure the following sets of options:

- Popular Settings
- Display Settings
- Scheduling Settings
- File Search Settings
- E-Mail Settings
- Hidden Web Data Search Settings
- Worldwide Search Settings
- Registry Search Settings
- AnyFind Settings
- Security Settings
- Logging Settings
**General Settings**

**Popular Settings Page**

The *Popular* settings page allows you to modify various options for Identity Finder. To open or modify these options, click the *Settings* button on the *Tools and Options* ribbon, and select *Popular* from the menu on the left.

The following options are available:

- Associating Identity Finder with Results Files
- Enabling Windows Explorer Shell Extensions
- Giving Other Programs Priority Over Identity Finder
- Resetting Message Box Confirmations
- Saving and Loading Identity Match Data on Startup and Exit
- Save Search Settings on Exit
- Enabling the Startup Wizard When You Open Identity Finder
- Enabling Autorecover
- Check for New Versions and Updates on Startup
Associating Identity Finder with Results Files

The *Associate Identity Finder with Results Files (*.idf)* setting enables Windows Explorer to recognize *.idf files as Identity Finder results. When enabled, you may double-click *.idf files in Windows and have them automatically open in Identity Finder. This will also display an Identity Finder results file icon for *.idf files in Windows Explorer.

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Giving Other Programs Priority Over Identity Finder

If enabled, the *Give Other Programs Priority Over Identity Finder* setting lowers the priority of Identity Finder's processes and threads to give precedence to your other Windows applications. Identity Finder will continue running and will be searching as fast as possible when you are not using your computer, but performance will be slightly slower when you are using other applications.

If Identity Finder is slowing your system performance or you other applications are too slow while Identity Finder is running, then check this box and click OK. You can change this setting at any time before or during a search.

If you would like Identity Finder to stop using any system resources, you can *Pause* the search and *Resume* it when you have completed your current task.

To view or change these settings, click the *Settings* button on the *Tools and Options* ribbon.
Resetting Message Box Confirmations

Identity Finder messages frequently provide you with options such as "Don't ask me again" or "Don't show this again" or "Always perform my selection" to allow advanced users to reduce the number of confirmations and messages your receive while taking actions on your identity matches. For example, when you Shred a file, Identity Finder will ask you to confirm that you wish to shred that file and provide you with the opportunity to turn off future confirmations. Clicking the Reset button will reset all message box confirmation dialogs so you are prompted again with all messages and warning.

To view or change these settings, click the Settings button on the Tools and Options ribbon.
Scheduling Identity Finder to Automatically Run

When enabled, the **Automatically Run Identity Finder Periodically** setting allows Identity Finder to automatically execute based on the schedule you specify. By default, if you do not specify a schedule, Identity Finder will run every Saturday night at 11:00pm.

To specify a different schedule, click the **Configure** button to open the **Configure Scheduled Task** dialog box.

First, choose **Schedule Task** and specify how often and when the task will execute:

Second, choose your **Search Options** for what to search for and where to search:

Note each of the features below are described in detail on their **Settings** pages.
### General settings

- Give other programs priority over Identity Finder
- Automatically exit Identity Finder after search completion

### What to search for

- Credit Card Numbers
- Bank Account Numbers
- Social Security Numbers
- Passwords

### Where to search

- Files
- Compressed Files
- E-Mail Messages
- E-Mail Attachments
- Hidden Web Data
- Windows Registry

**File locations:**
- Documents and Settings
- Computer
- Custom location(s): [Select Folders]

### File search settings

Search files of the following types:
- Search only common files
- Search all filterable files
- Search all files

- Search only files modified since: 10/15/2007
- Use search history and only search new or modified files

### E-Mail search settings

- Search only e-mails modified since: 10/15/2007
- Use search history and only search new or modified e-mails

### Results

- Automatically save results with secure password

**File location:**

- Create the specified folder if it does not exist:
  - Enter password: ********
  - Confirm password: ********
- Automatically save a copy of results to a second location

**File location:**

- Create the specified folder if it does not exist:
  - Enter password: ******
  - Confirm password: ******
Third, when you click **OK** or **Apply**, you must type in the username and password you use to log into Windows.

Note: When you schedule a task in Windows, it requires your user name and password to allow that program to run as you. Identity Finder does not store your username and password, rather it simply passes them to the Windows system. When you click **OK** or, if you click **Set Password** in the Advanced options, you will see the Scheduled Task Account Settings dialog box:

![Scheduled Task Account Settings](image)

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Export Scheduled Task Search Settings

This feature is only available in Enterprise Edition.

The Export a Configuration Settings file for use on any computer setting allows a power user or administrator to export schedule task search settings as a Configuration Settings (*.ini) file. This file may then be copied to other computers and supplied to Identity Finder for a completely customized execution. This feature makes it very easy to configure Identity Finder from a centralized administrator workstation and then use those settings to customize the execution of Identity Finder on remote computers.

To export search settings, first select the Export a Configuration Settings file for use on any computer radio button. If you want to import previous exported Configuration settings, you can click the Import button and choose your file. You may also copy settings from your current configuration by clicking the Copy button.

Second, choose your Search Options for what to search for and where to search (Note each of the features below are described in detail on their Settings pages):
### General settings

- Give other programs priority over Identity Finder
- Automatically exit Identity Finder after search completion

### What to search for

- Credit Card Numbers
- Bank Account Numbers
- Social Security Numbers
- Passwords

### Where to search

- Files
- Compressed Files
- E-Mail Messages
- E-Mail Attachments
- Hidden Web Data
- Windows Registry

**File locations:**
- Documents and Settings
- Computer
- Custom location(s): [Select Folders]

### File search settings

- Search files of the following types:
  - Search only common files
  - Search all filterable files
  - Search all files
- Search only files modified since: 10/15/2007
- Use search history and only search new or modified files

### E-Mail search settings

- Search only e-mails modified since: 10/15/2007
- Use search history and only search new or modified e-mails

### Results

- Automatically save results with secure password
- Create the specified folder if it does not exist:
- Enter password: [Passwords]
- Confirm password: [Passwords]
- Automatically save a copy of results to a second location
- File location:
- Create the specified folder if it does not exist:
- Enter password: [Passwords]
- Confirm password: [Passwords]
Finally, click the *Export* button to save your settings to a configuration file. You will be prompted for a location to save your *Configuration Settings (*.ini) file*. Note: When the *Export a Configuration Settings file for use on any computer* radio button is selected, the *OK* and *Apply* buttons will not save the specified settings.

To view or change these settings, click the *Settings* button on the *Tools and Options* ribbon.

**Scheduling a Task Using Your Configuration Settings File**

To schedule Identity Finder to run with your Configuration Settings file setting, schedule the following task to run:

```
identityfinder.exe /jobmode /inifile=c:\full path to\filename.ini
```

See Also: [Command Line Parameters and Execution of Identity Finder](#)
**Startup/Exit Settings**

**Scheduling Settings Page**

The *Scheduling* settings page allows you to modify the scheduling options for Identity Finder. To open or modify these options, click the *Settings* button on the *Tools and Options* ribbon, and select *Scheduling* from the menu on the left.

There are many options available to you. See the following topics to learn more:

- [Scheduling Identity Finder to Automatically Run](#)
- [Export Scheduled Task Search Settings](#)
Advanced Settings to Customize Your Experience

Identity Finder

Popular
Display
Scheduling
File Search
E-Mail Search
Hidden Web Data Search
Registry Search
Worldwide Search
AnyFind
Security
Logging

Customize the options for scheduling Identity Finder

Scheduling Identity Finder to run automatically

- Do not schedule Identity Finder
- Schedule Identity Finder using your configuration: Configure
- Export a Configuration Settings file for use on any computer: Export
- Replace all settings below with current configuration: Copy

General settings

- Give other programs priority over Identity Finder
- Automatically exit Identity Finder after search completion

What to search for

- Credit Card Numbers
- Bank Account Numbers
- Social Security Numbers
- Passwords

Where to search

- Files
- Compressed Files
- E-Mail Messages
- E-Mail Attachments
- Hidden Web Data
- Windows Registry

File locations:

- Documents and Settings
- Computer
- Custom location(s): Select Folders

File search settings

Search files of the following types:

- Search only common files
- Search all filterable files
- Search all files

- Search only files modified since: 10/15/2007
- Use search history and only search new or modified files

E-Mail search settings

- Search only e-mails modified since: 10/15/2007
- Use search history and only search new or modified e-mails

Results

- Automatically save results with secure password

File location:

- Create the specified folder if it does not exist
- Enter password: **********
Advanced Settings to Customize Your Experience
Saving and Loading Personal Information File on Startup and Exit

If enabled, the **Load Personal Information File on Startup** setting automatically loads your Personal Information File, which contains your Unique Identity Include List and your Identity and Location Ignore List, when Identity Finder starts. You will be prompted for your password during this process.

If enabled, the **Save Personal Information File on Exit** setting automatically saves any changes you made to your Personal Information File when you exit Identity Finder.

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Enabling the Startup Wizard When You Open Identity Finder

If enabled, the *Enable Identity Finder Wizard on Startup* setting will cause Identity Finder to open with the Startup Wizard each time you run the program. If you decide you do not want to use the wizard, uncheck this box. If you previously disabled the Startup Wizard and now want it to open each time you run Identity Finder, you must check this box.

You can also access the Startup Wizard at any time by clicking the *Wizard* button on the Main ribbon.

To view or change these settings, click the *Settings* button on the *Tools and Options* ribbon.
Enabling Autorecover

When enabled, the **Enable Autorecover on Startup** setting allows Identity Finder to periodically, automatically save your results into an encrypted file. If Identity Finder is terminated abruptly due to a system restart, power loss, or for any other reason, next time you start Identity Finder, you will have the option to load any saved results. If you load the results, take action on the items, and also use the default **Search Only Files Modified Since Last Search Run** option, you will save a great deal of time when you resume your previous incomplete search by selecting the same options as before and clicking Start.

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Saving Search Settings on Exit

If enabled, the *Save Search Settings on Exit* setting automatically saves the following information when Identity Finder exits (and will automatically load these settings when Identity Finder starts):

- **AnyFind**: Saves the selected or deselected state of the AnyFind identity type buttons on the What to Search for ribbon
- **Where to Search**: Saves the selected or deselected state of all buttons on the Where to Search ribbon
- **Quick Access**: Saves the buttons you have configured to be displayed in the Quick Access Menu

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Checking for New Versions and Updates

When enabled, the *Check for New Versions and Updates on Startup* setting allows Identity Finder to automatically check the identityfinder.com server on the internet to see if a new version or upgrade to the application or *AnyFind Definitions* are available for your installation of Identity Finder. *No personal information is sent at this time by Identity Finder.*

You can also check for a new version or update immediately by clicking the *Check Now* button on this page or by clicking the *Check for Updates* button on the *Tools and Options* ribbon.

If a new version of Identity Finder is available, you will be prompted to download and either save or install the upgrade. You will not need to reactivate Identity Finder, if you install over your existing version in the same folder. You will need to restart Identity Finder.
If a new version of AnyFind Definitions is available, you will be prompted to download the upgrade. This download will automatically install the new definitions does not require you to restart Identity Finder.

If there is an error while downloading an update, you may be directed to manually download the update from the URL specified in the error message. This URL will contain a link to the file you should download as well as instructions on installing the update.

To view or change these settings, click the Settings button on the Tools and Options ribbon.
User Interface Settings

Display Settings Page

The *Display* settings page allows you to modify visual options for Identity Finder. To open or modify these options, click the *Settings* button on the *Tools and Options* ribbon, and select *Display* from the menu on the left.

The following options are available:

- Showing the System Tray Icon and Balloon Tips
- Enable Word Wrap in Preview Pane
- Specify the Number of Identity Matches Found and Displayed in each Location
- Mask Identity Matches
**Showing the System Tray Icon and Balloon Tips**

If enabled, the *Show System Tray Icon* setting creates an icon in the Windows system tray in the bottom right of your taskbar. *Identity Finder’s system tray icon* gives you quick access to several commands before, during, and after a search.

If enabled, the *Show Tray Balloon Tips* setting adds popup balloon notifications to the system tray icon to alert you of progress and status. This option is only available when the *Show System Tray Icon* setting is enabled.

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Enabling Word Wrap in Preview Pane

If enabled, the *Enable Word Wrap in Preview Pane* setting will allow words on the same line of a file to be automatically moved to the beginning of the next line of the preview pane if the width of the preview pane window is not wide enough. By default this setting is enabled, but you might want to turn it off for certain files that have precise formatting in them.

To view or change these settings, click the *Settings* button on the *Tools and Options* ribbon.
Specify the Number of Identity Matches Found and Displayed in each Location

The Specify the Number of Identity Matches found Displayed in each Location setting allows you to specify the maximum number of matches displayed in the results view, as well as whether Identity Finder should stop searching the current location once it reaches a maximum match count. By default in Home and Professional Editions, this setting is enabled to perform a complete search and display all the matches in each location. In Enterprise Edition, this setting is enabled to perform a complete search of each location but to display a maximum of 99 matches per location. You might want to enable a different option depending on your needs for reporting or speed and performance.

There are three options:

- Complete search: Identity Finder will search a location completely and list every match found.
- Complete with partial view: Identity Finder will search a location completely and display the total count of all matches found, but it will not list every match found individually. Summary reports will be accurate, but only the first Maximum Matches will be listed individually in your report. This option is best when you have locations with many matches as it will make analyzing your results easier. This option also improves memory performance over complete search.
- Partial search: Identity Finder will search a location until it finds the first Maximum Matches in that location. It will then skip to the next location. This can greatly improve performance if you have locations with many matches. Note: all locations will be accurately identified but not all matches will be listed. This option improves memory and speed performance over Complete with partial view.

**Maximum Matches** is the threshold that specifies when the bottom two options become active. This threshold dictates when Identity Finder will restrict the number of identity matches found or displayed.

Below is an example of what restricting the number of identity matches will look like when Complete with partial view is selected. It is displaying only the first 10 matches because more than 10 were found:
To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Security Settings

Security Settings Page

The Security settings page allows you to modify security options for Identity Finder such as password strength requirements. To open or modify these options, click the Settings button on the Tools and Options ribbon, and select Security from the menu on the left.

The following options are available:
- Change Your Saved Password for the Personal Information File
- Deleting Your Personal Information File
- Password Strength Requirements [Professional/Enterprise]
- Quarantine Location [/Enterprise]
- Redact From Text Files [Professional/Enterprise]

Note: The Password strength requirements feature and Redact feature are only available in Professional and Enterprise editions. The Quarantine feature is only available in Enterprise edition.
Change Your Saved Password for the Personal Information File

Identity Finder uses a single master password to securely store all your personal information related to Identity Finder inside a Personal Information File. Personal Information related to Identity Finder includes your Unique Identity Include List, Identity and Location Ignore List, Password Vault, and if using Enterprise Edition your Network Credentials. Identity Finder will let you save all this information in an encrypted format with a password. If you want to change your password, press the Change button.

Once you press the Change button, you will be required to enter your current password and then your new password twice.
Note: If you have not saved any information related to Identity Finder, you won't have a Personal Information File password. In this case, the Change button will be gray.

To view or change these settings, click the Settings button on the Tools and Options ribbon.
Configuring Password Strength Requirements

This feature is only available in Professional and Enterprise Editions.

If enabled, the Password Strength Requirements setting will force all passwords entered within the Identity Finder application to be strong. The following options can be set:

- Do Not Require Strong Passwords: Passwords can be any length and contain any characters.
- Require Strong Passwords: Passwords must be at least six characters and contain at least one letter and one non-letter.
- Require Stronger Passwords: Passwords must be at least eight characters and contain at least three of the following four types of characters:
  - Lowercase letters
  - Uppercase letters
  - Numbers
  - Symbols (i.e., !@#$%^&*:;/, etc.)

To view or change these settings, click the Settings button on the Tools and Options ribbon.
Configuring Quarantine Location

This feature is only available in Enterprise Edition.

When set, the Quarantine Location specifies where the default location for a file you decide to quarantine will be securely moved. This location should be a secure folder on your computer, such as an encrypted drive or one to which unauthorized individuals cannot gain access. If you choose the Leave Behind Warning Text Document in Place of File then a text file will be created in its place named exactly the same as the original file including its extension but with a .txt appended to the end. If your file was c:\test.doc then a file c:\test.doc.txt will be left in its place after it is quarantined.

The text file is useful to notify the original file owner that you moved their file securely. Here is a sample of the text:
The original file, c:\test.doc, contained unsecured, personally identifiable information. It has been quarantined to: d:\test.doc

To view or change these settings, click the Settings button on the Tools and Options ribbon.
**File Search Settings**

**File Search Settings Page**

The File Search settings page allows you to modify options for how Identity Finder searches files. To open or modify these options, click the Settings button on the Tools and Options ribbon, and select File Search from the menu on the left or click the Files button on the Where to Search ribbon and select the Configure Search Settings option.

The following options are available:

- Searching Only Common Files versus Some or All Files
- Manage Custom File Type List
- Override Default Search Filters
- Searching Only Files Less than User Specified Size
- Searching Only Files Created/Modified Since User Specified Date
- Searching Only Files New/Modified Since Last Search
- Allowing Prompt for Network Credentials
- Including Mapped Network Drives In Search
- Including Custom Folder List when searching Remote Computers
- Allow Searching of File systems Not Fully Supported by Microsoft Windows
Searching Only Common File Types, Filterable File Types, Custom File Type List, or All Files

With the Search the following file types using Identity Finder option you have the option to let Identity Finder search only common file types, all filterable file types, or all files:

- **Search Only Common File Types (this is the default option):** This option will perform the quickest search while also searching the files on your computer most likely to contain personal information. When this option is selected, Identity Finder will search though text files (including most Instant Messenger logs), Microsoft Office files, Adobe Acrobat PDF files, web page documents (such as HTML files), and other common formats. Even if your computer has the ability to search metadata stored within a file – such as when a photo was taken for a jpg file or the artist information in an mp3 file – that information will not be searched when this option is selected.

- **Search All Filterable File Types:** This option searches through all files that your computer has the ability to search via an internal Identity Finder filter or via a Windows IFilter. When this option is selected, Identity Finder will search all common file types plus any other file type for which you have installed an IFilter. For example, if your camera software installed the ability for Windows to read information from a jpg file about when a photo was taken or a drawing program installed the ability for Windows to read the text from shapes and other visual elements, then that information will also be searched.

- **Search Custom File Types [Professional and Enterprise Editions]:** This option allows you to select the files that Identity Finder will search. For more information, please see Manage Custom File Type List.

- **Search All Files [Professional and Enterprise Editions]:** This option is the slowest option because Identity Finder will try and extract all the text from any type of file that does not have an internal Identity Finder filter or an IFilter. No matter what type of file or what the file is named, when this option is selected, Identity Finder will search inside of it.
To allow Identity Finder to search files for which you have installed an IFilter, you must select the *All filterable file types, Custom file type list*, or *Search all files* radio button. Note: If you would like to override the default filter that is used for searching files click the *Override* button. For example, you might want to add additional extensions to be considered text, such as *.bak*. In this case you may override default search filters so that those file types are treated as text. See the *Override Default Search Filters* help topic for more information. Note: Identity Finder does not interpret audio or video, therefore a picture of a password or a song with lyrics about your password will not be found.

To view or change these settings, click the *Settings* button on the *Tools and Options* ribbon.
Searching Only Files Less than User Specified Size

The *Search Files Only Less than this Size* setting prevents Identity Finder from searching any files that are greater in size than the number of megabytes (MB) specified. This feature enables you to increase the speed and performance of Identity Finder's search and is especially useful when searching folders containing large documents that contain only images.

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
**Searching Only Files Created/Modified Since User Specified Time**

This feature is only available in Professional and Enterprise Editions.

If enabled, the *Search Only Files Created or Modified Since the Following Date (MM/DD/YYYY)* setting prevents Identity Finder from searching any files that have not changed since the date specified. This feature enables you to increase the speed and performance of Identity Finder's search and is especially useful if you recently ran Identity Finder but did not have the *Searching Only Files Created/Modified Since Last Search* option enabled and only wish to search files modified since that previous search.

To view or change these settings, click the Settings button on the Tools and Options ribbon.
Searching Only New/Modified Files Since Last Search

If enabled, the Use Search History and Only Search New or Modified Files setting enables you to increase the speed and performance of Identity Finder's search by skipping any files already searched by Identity Finder that have not been modified since your previous search.

The first time you run a search after you enable this checkbox, a search history database will be created with information about all of files that Identity Finder searches. Each additional time you run a search with this checkbox enabled, Identity Finder will skip all files that have not changed since the previous search as long as they did not contain any Identity Matches. Files found to contain Identity Matches during a search will be searched again on later searches unless you specifically add those files to the Ignore Identities and Locations list.

If you modify your AnyFind settings or Include Unique Identities then you should Delete your database to ensure that all Files are searched again and a new database is created. Additionally, if you use the Hidden Web Data features of your web browser and new items are added, your unchanged Files will not be searched for this new information unless you delete your databases. Therefore, to always ensure maximum comprehensiveness, you should delete your database on the noted occasions.
To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
**E-Mail Search Settings**

**E-Mail Settings Page**

The *E-Mail Search* settings page allows you to modify the Outlook, Outlook Express, and Windows Mail options for Identity Finder as well as how Identity Finder searches E-Mail. To open or modify the options, click the *Settings* button on the *Tools and Options* ribbon, and select *E-Mail Search* from the menu on the left. Alternatively you may click the *Messages* button on the *Where to Search* ribbon and select the *Configure Search Settings* option.

The following options are available:

- Include Outlook and Exchange in E-Mail Search
- Search Exchange Mail Server Folders [Professional/Enterprise]
- Search All or Only Specified Mail Folders
- Select Outlook and Exchange Folders
- Searching Additional Outlook Data Files
- Include Outlook Express or Windows Mail in E-Mail Search
- Searching Only E-Mails Created/Modified Since User Specified Time
- Searching Only New/Modified E-Mails Since Last Search
Including Outlook and Exchange in E-Mail Search

If enabled, the *Include Outlook and Exchange in E-Mail Search* setting will enable Identity Finder to search within your local Outlook folders and any available remote Exchange Server folders. You must select this option in order to be able to modify the other Outlook settings below it.

To view or change these settings, click the *Settings* button on the *Tools and Options* ribbon.
Searching Remote Mail Folders

This feature is only available in Enterprise edition.

If enabled, the Search remote mail folders setting will enable Identity Finder to search within all the folders connected via a Microsoft Exchange Mail Server or via IMAP.

Note: Disabling this option will prevent Identity Finder from searching any local Outlook Folders that are also connected to an Exchange Server.

To view or change these settings, click the Settings button on the Tools and Options ribbon.
Searching All or Only Specified Mail Folders

This feature is only available in Professional and Enterprise editions.

With the *Search all available folders* setting you can choose to have Identity Finder automatically search within all available folders that it finds, including those on an Exchange Server (if you enabled the *Searching Remote Mail Folders* option), or with the *Search only specified folders settings* you can choose to have Identity Finder search only within the specific folders you specify.

If you wish to search within only the specific folders that you specify, click the *Select Folders* button to open the *Select Outlook and Exchange Folders* dialog box. Please be patient while this dialog box opens as it will be retrieving the entire list of folders that it is possible to search.

To view or change these settings, click the *Settings* button on the *Tools and Options* ribbon.
Select Outlook and Exchange Folders

This feature is only available in Professional and Enterprise editions.

The Select Outlook and Exchange Folders dialog box allows you to select which folders Identity Finder will search. Please be patient while this dialog box opens as it will be retrieving the entire list of folders that it is possible to search. In this window you will see a list of all local Outlook folders and, if you enabled the Search Exchange Mail Server Folders option, you will also see all your folders that exist remotely on Exchange Servers or via IMAP connections.

To help you identify each folder, the Profile name, Store name, and Folder name are listed. Click the checkbox next to each Folder you want to search. If you later add folders within Outlook, they will automatically be checked and included in your next search.

For quick and easy selection of multiples folders or multiple stores, you can use the Select All and Deselect All buttons. The buttons you may use are:

- **For all folders in all stores in all profiles**: To select or deselect every folder that you can search across all stores and profiles.
- **For all folders in all stores in the currently highlighted profile**: To select or deselect every folder within the profile your focus is on regardless of which store they are within inside that profile.
- **For all folders in the currently highlighted store**: To select or deselect every folder within the store your focus is on.

To view or change these settings, click the Settings button on the Tools and Options ribbon.
Advanced Settings to Customize Your Experience
Include Outlook Express or Windows Mail in E-Mail Search

If enabled, the *Include Outlook Express or Windows Mail in e-mail search* setting will enable Identity Finder to search within your local Outlook Express or Windows Mail folders.

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Searching Only E-Mails Created/Modified Since User Specified Time

This feature is only available in Professional and Enterprise Editions.

If enabled, the Search Only E-Mails Created or Modified Since the Following Date (MM/DD/YYYY) setting prevents Identity Finder from searching any E-Mails that have not changed since the date specified. This feature enables you to increase the speed and performance of Identity Finder’s search and is especially useful if you recently ran Identity Finder but did not have the Searching Only E-Mails Created/Modified Since Last Search option enabled and only wish to search E-Mails modified since that previous search.

To view or change these settings, click the Settings button on the Tools and Options ribbon.
Searching Only New/Modified E-Mails Since Last Search

If enabled, the *Use Search History and Only Search New or Modified E-Mails* setting enables you to increase the speed and performance of Identity Finder’s search by skipping any E-Mails already searched by Identity Finder that have not been modified since your previous search.

The first time you run a search after you enable this checkbox, a search history database will be created with information about all of the E-Mails that Identity Finder searches. Each additional time you run a search with this checkbox enabled, Identity Finder will skip all messages that have not changed since the previous search as long as they did not contain any Identity Matches. E-Mails found to contain Identity Matches during a search will be searched again on subsequent searches unless you specifically add those messages to the *Ignore Identities and Locations* list.

If you modify your *AnyFind* settings or *Include Unique Identities* then you should Delete your database to ensure that all E-Mails are searched again and a new database is created. Additionally, if you use the *Search All Locations for Passwords found in Hidden Web Data* setting and new items are added, your unchanged E-Mails will not be searched for this new information unless you delete your databases. Therefore, to always ensure maximum comprehensiveness, you should delete your database on the noted occasions.
To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Hidden Web Data Search Settings

Hidden Web Data Search Settings Page

The *Hidden Web Data Search* settings page allows you to modify options for how Identity Finder searches Hidden Web Data. To open or modify these options, click the *Settings* button on the *Tools and Options* ribbon, and select *Hidden Web Data Search* from the menu on the left. Alternatively you may click the *Hidden Web Data* button on the *Where to Search* ribbon and select the *Configure Search Settings* option.

The following options are available:

- Include Internet Explorer in Search
- Include Firefox in Search
- Search All Locations for Passwords found in Hidden Web Data
Include Internet Explorer in Search

If enabled, the *Include Internet Explorer in Search* setting will enable Identity Finder to search for saved passwords and AutoComplete form data within Internet Explorer.

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Include Firefox in Search

If enabled, the *Include Firefox in Search* setting will enable Identity Finder to search for saved passwords and form data form data within Firefox. Choose *Search Firefox Passwords* to enable searching of passwords and choose *Search Firefox Form Data* to enable searching for form data.

To view or change these settings, click the **Settings** button on the *Tools and Options* ribbon.
Search All Locations for Passwords found in Hidden Web Data

If enabled, the **Search All Locations for Passwords found in Hidden Web Data** setting will enable Identity Finder to search all other locations for passwords that were found during the Hidden Web Data search. This will increase the length of time it takes to perform a search, but is more comprehensive. If you have a common phrase such as your e-mail address as a saved password, there could be a large number of false positives reported during your search. To reduce these false positives, you may **ignore the Identity Match**.

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
**Worldwide Search Settings**

**Worldwide Search Settings Page**

The *Worldwide Search* settings page allows you to enable the ability to perform Worldwide searching of personal information from additional countries. To open or modify the options, either click the *Settings* button on the *Tools and Options* ribbon and select *Worldwide Search* from the menu on the left.

The following options are available:

- Enabling Worldwide Searching

![Customize worldwide search settings]

- *Australia*
  - Enable "Tax File Number (TFN)" search

- *Canada*
  - Enable "Social Insurance Number (SIN)" search

- *United Kingdom*
  - Enable "National Insurance Number (NINO)" search
  - Enable "National Health Service Number (NHS Number)" search
Enabling Worldwide Searching

Worldwide searching is a feature available within Identity Finder to search for personal information from additional countries. By enabling any of the four new Identity Match Types, AnyFind Worldwide Searching for that identity type will be enabled and turned on for your next search. You may also manually enable Unique Searching of these identity types and Add Unique Identity information.

To modify Worldwide searching, either click the Settings button on the Tools and Options ribbon and select Worldwide Search from the menu. You can also select what Worldwide Identity Match Types you want to enable:

- **Australia**: Tax File Number (TFN)
- **Canada**: Social Insurance Number (SIN)
- **United Kingdom**: National Insurance Number (NINO)
- **United Kingdom**: National Health Service Number (NHS Number)

To view or change these settings, click the Settings button on the Tools and Options ribbon.
Network Search Settings

Registry Search Settings Page

The Registry Search settings page allows you to modify the options for the searching of the Windows Registry. To open or modify these options, click the Settings button on the Tools and Options ribbon, and select Registry Search from the menu on the left. Alternatively you may click the Registry button on the Where to Search ribbon and select the Configure Search Settings option.

The following options are available:

- Searching Only Common Keys versus All Keys
Allowing Prompt for Network Credentials

This feature is only available in Enterprise Edition.

If enabled, the Allow Prompt for Network Credentials During Search setting will allow Identity Finder to pop up a dialog box and prompt you for the credentials of a remote computer. The prompt will only occur if Identity Finder cannot connect to the remote machine via existing or supplied credentials. Identity Finder will attempt to connect to all specified remote computers at the beginning of the search, so, all necessary prompts for all computers will appear shortly after starting the search. However, if you want to guarantee that the search will run without user interaction, you should disable this checkbox.

To view or change these settings, click the Settings button on the Tools and Options ribbon.
AnyFind Settings

AnyFind Settings Page

The AnyFind settings page and all its content is only available in Professional and Enterprise editions.

The AnyFind settings page allows you to modify how Identity Finder automatically searches for personal information. To open or modify these options, click the Settings button on the Tools and Options ribbon, and select AnyFind from the menu on the left.

The following options are available:

- Searching for Unformatted Social Security Numbers
- Requiring Keywords for Unformatted Social Security Numbers
- Using Custom Keywords to Find Unformatted SSNs
- Requiring a Minimum Amount of Social Security Numbers
- Allowing Non-Printable Characters in Passwords
- Comprehensive Password Searching
- Finding Dates of Birth with AnyFind
Searching for Unformatted Social Security Numbers within Locations

This feature can only be modified in Professional and Enterprise Editions.

You can specify for Identity Finder to Search for unformatted SSNs in locations. Unformatted Social Security Numbers (SSNs) are numbers in locations without dashes or spaces or other characters. For example, 123456789 could be an unformatted SSN. There are three options:

- **Never search for unformatted SSNs:** Identity Finder will always ignore unformatted SSNs unless there is an SSN keyword near the number (for example: "SSN: 123456789").
- **Only search for unformatted SSNs in Excel and CSV files:** Identity Finder will search inside Excel spreadsheets and CSV files for unformatted SSNs but will ignore unformatted SSNs in all other locations.
- **Always search for unformatted SSNs (this is the default option):** Identity Finder will search all locations for unformatted SSNs. This may yield a high number of false positive results because nine digit numbers are common, therefore, there are additional options to help reduce the number of false positives.

Select the radio button of your preference.

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Requiring Keywords for Unformatted Social Security Numbers

The Unformatted SSN features can only be modified in Enterprise Edition.

If enabled, the Only Match Unformatted SSNs When Location Contains Keyword setting will require Identity Finder to also locate a keyword (i.e., SSN, Social Security Number, SS#, etc.) anywhere within the result location. This option is enabled by default and helps to eliminate many false positives.

To view or change these settings, click the Settings button on the Tools and Options ribbon.
**Requiring a Minimum Amount of Social Security Numbers**

*This feature can only be modified in Enterprise Edition.*

If enabled, the **Only Match Unformatted SSNs When Location Contains at Least this Many Unformatted SSNs** setting will require Identity Finder to locate the specified minimum number of unformatted SSNs. Often times, locations will contain unformatted SSNs in the form of a list. This settings is valuable for eliminating locations that contain only a single (or other specified number) of unformatted nine digit number(s) that might not represent a list of SSNs. This setting is set to 3 by default and therefore requires that at least 3 unformatted SSNs be found in a location before considering them to be valid.

![Identity Finder Settings](image)

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Comprehensive Password Searching

This feature can only be modified in Professional and Enterprise Editions.

With the **Enable comprehensive searching for passwords in the following file types** setting you can specify when Identity Finder will comprehensively search for passwords in files. When **AnyFind Passwords** is enabled, Identity Finder will search all locations you specify for passwords, but comprehensive searching is a more in-depth searching algorithm that sometimes yields more false positives especially in audio and visual files like mp3 and jpg files. You can choose to only allow comprehensive searching to occur on **Filterable** files (usually includes documents, spreadsheets, or all files). Comprehensive searching will always occur in locations other than files (such as E-Mails and System Areas).

- **None (Do Not Enable Comprehensive Searching Anywhere):** Identity Finder will not perform in-depth comprehensive searching of passwords in any file types. It will only find passwords using standard techniques.
- **Enable Comprehensive Searching Only in Filterable File Types (this is the default setting):** Identity Finder will only perform in-depth comprehensive searching of passwords in Filterable files types.
- **Enable Comprehensive Searching in All File Types:** Identity Finder will perform in-depth comprehensive searching of passwords in all files types.

Select the radio button of your preference.

To view or change these settings, click the **Settings** button on the **Tools and Options** ribbon.
Logging Settings

Logging Settings Page

The Logging settings page allows you to modify the options for Identity Finder. To open or modify the options, either click the Settings button on the Tools and Options ribbon and select Logging from the menu on the left. Alternatively you may click the Logging button on the Tools and Options ribbon and select the Configure Log Settings option.

The following options are available:

- Enable Logging
- Enable Log Security [Professional/Enterprise]
Note: The Log Security feature is only available in Professional and Enterprise editions.
Enabling Logging

Logging is a feature available within Identity Finder to record detailed information about your search. A file is created in the Logs subfolder of your user’s Identity Finder local application data folder (i.e., C:\Users\username\AppData\Local\Identity Finder\Identity Finder Edition\logs) with the name IDF_DATE_TIME.log. The logs provide you with information for the specific categories that you specify.

You can choose to enable or disable logging and the folder where the log will be stored. Additionally, you can choose whether to create a new log file every time Identity Finder is opened (each session), or to append to a single log file. The file may be tab separated, comma separated, or fixed width.

You can also select what types of information you want logged to your file:

- Items Searched
- Matching Items
- Secure Items Skipped
- User Actions
- Messages
- Errors
If you want to delete all contents of the log folder you have specified, you may press the Clear Logs button.

To view or change these settings, click the Settings button on the Tools and Options ribbon.
Enabling Log Security

This feature is only available in Professional and Enterprise Editions.

The Enable Encryption setting allows you to have all log files created by Identity Finder encrypted so that they may not be read outside the Identity Finder application.

To view or change these settings, click the Settings button on the Tools and Options ribbon.

To view an encrypted Log:
Click the Logging button on the Tools and Options ribbon and select the View Current Log option or View Any Log option.
Advanced Settings to Customize Your Experience
Tools to Secure Your Identity

What are the Identity Finder Tools?

Identity Finder Tools provide additional features to help you prevent identity theft independent of your search results. There are seven tools that allow you to protect and shred personal information located on your computer:

- **Password Vault Tool** - This allows you to securely store usernames and passwords for websites, encrypted files, and other locations inside of Identity Finder.
- **Secure File Tool** - This allows you to secure any file on your computer even if no Identity Match is found in that file.
- **Open Secure Zip File Tool** - This allows you to open any secure zip file on your computer and extract the contents.
- **Shred File or Folders Tool** - This allows you to shred any file or folder on your computer even if no Identity Match is found in that file.
- **Secure Microsoft IE Tool** - This allows you to secure your configuration settings Internet Explorer so personal information and passwords are not saved.
- **Shred Microsoft Internet Explorer Locations Tool** - This allows you to shred your Internet Explorer Temporary Internet Files, Cookies, History, Form Data, and Passwords.
Tools to Secure Your Identity

- **Secure Firefox Tool** - This allows you to secure your configuration settings for Firefox so that passwords are protected and personal information is not saved.
- **Shred Firefox Locations Tool** - This allows you to shred your Firefox Browsing History, Download History, Saved Form and Search History, Cache, Cookies, and Saved Passwords.

You may also access all the tools via the "Tools and Options" ribbon.
Password Vault Tool

The Password Vault tool allows you to securely store and manage usernames and passwords for websites, encrypted files, and other locations inside of Identity Finder and protect them with a single, master password. The master password is the same password you use to secure other personal information within Identity Finder.

There are two ways to access the Password Vault tool:

1. Click the Password Vault button on the Tools and Options ribbon.
2. Click the Application Menu button in the upper left corner of Identity Finder, then highlight Tools, then highlight and left-click "Password Vault..."

Managing Passwords

Once selected, the Password Vault dialog will open. Enter any Location, Comment, Username, and/or Password then click Add. After entering your master password, your information will be stored securely. At no point does Identity Finder attempt to validate that the usernames or passwords that you place in the password vault are correct, therefore, it is necessary for you to ensure that you type them in correctly.
**Adding Passwords from Identity Finder**

When you are performing a search you can add passwords into your Vault very quickly. If you right-click on a Hidden Web Data password result, the menu includes the option to "Add to Password Vault." Selecting this action will copy the selected location, username, and password into the Password Vault. This action does not delete the Hidden Web Data, so you should make sure to also click the "Shred" button, if you do not want someone else to be able to obtain this password.

When you are performing Secure actions like encrypting a document with a password, you can add passwords you create into your Vault very quickly. Simply click the "Securely store this password in your Password Vault" as depicted below:

![Identity Finder](image)

**Editing Existing Password Inside the Vault**

If you need to modify an existing entry of your Password Vault, simply highlight the entry in the top part of the Vault then click the Edit button. All the information will be moved into the edit fields below. After you have completed your changes do not forget to click the Add button so your password goes back into the Vault.

**Launching Applications from Your Password Vault**

If you would like to quickly and easily open a document or visit a website contained within your Password Vault, simply double click the highlighted entry. You may also click the Open button after highlighting an entry.

Note: All the information you enter will be saved to your Personal Information File (PIF). If you did not load this file on startup or you want to revert your changes to the last time you saved, you may press the "Load PIF" button. If you want your changes saved to your PIF, click the "Save PIF" button.

**Masking Passwords**

If you do not want your passwords displayed at all times to protect yourself from someone glancing over your shoulder to see them when the Vault is open, click the Mask button. To display your passwords, click Unmask.
Secure File Tool

The Secure File tool allows you to secure any file on your computer even if no Identity Match is found in that file. There are two ways to access the Secure File tool:

1. Click the Secure File button on the Tools and Options ribbon.
2. Click the Application Menu button in the upper left corner of Identity Finder, then highlight Tools, then highlight and left-click "Secure File..."

Once selected, the Secure File dialog will open. Click the File Selection button (...) to launch a dialog box that allows you to select any file on your computer. After navigating to your desired location, click the "Open" button and the full path to your selected file will be displayed. Then click "Secure" and you will be presented with the specific options to secure that type of file such as encryption strength and password. Choose the appropriate options and click OK to secure your file.
Open Secure Zip File Tool

The Open Secure Zip File tool allows you to open and extract (unzip) the contents of any secure zip file on your computer. This is a very useful feature if you used Secured a Compressed File or Secured a Text Based or Other File in conjunction with the Strong or Stronger encryption setting. There are two ways to access the Open Secure Zip File tool:

1. Click the Open Secure Zip File button on the Tools and Options ribbon.
2. Click the Application Menu button in the upper left corner of Identity Finder, then highlight Tools, then highlight and left-click "Open Secure Zip File..."

Once selected, the Open Secure Zip File dialog will open. Click the Select Zip File button to launch a dialog box that allows you to select any zip file on your computer. After navigating to your desired location, click the "Open" button and the full path to your selected file will be displayed. Then click the Select Target Location button to launch a dialog box that allows you to select any folder on your computer. After navigating to your desired location, click the "OK" button and the full path to your selected folder will be displayed. Finally, type your password in the Password field and click the "Extract" button. Your files will be extracted to the desired location and an Explorer window will open to display the extracted files.
Tools to Secure Your Identity

**Shred Files or Folders Tool**

The Shred Files and Folders tool allows you to **shred** any file or folder (and all its subfolders and files) on your computer, even if no Identity Match is found in the specified file(s). There are two ways to access the Shred Files and Folders tool:

1. Click the Shred Files or Folders button on the Tools and Options ribbon.
2. Click the **Application Menu button** in the upper left corner of Identity Finder, then highlight Tools, then highlight and left-click "Shred Files and Folders..."

Once selected the Shred File(s) dialog will open. Click the Browse Selection button to launch a dialog box that allows you to select any file or folder on your computer. After navigating to your desired location, click the "OK" button and the full path to your selected file or folder will be displayed. Then click "Shred" and your file or folder will be shredded. **Note:** If you selected a folder, all of its files and subfolders within that folder will also be shredded.

**Note:** It is not possible to "undo" a Shred. Shredded results cannot be recovered. Once you shred something, it is gone.
Tools to Secure Your Identity

Secure Microsoft Internet Explorer (IE) Tool

The Secure Microsoft Internet Explorer (IE) tool allows you to easily configure Internet Explorer to be more secure. When Internet Explorer has saved sensitive passwords and form data and you wish prevent it from doing so in the future, you should utilize this tool. Internet Explorer AutoComplete data cannot be stored securely on your computer. There are two ways to access the Secure Microsoft IE tool:

1. Click the Secure Microsoft IE button on the Tools and Options ribbon.
2. Click the Application Menu button in the upper left corner of Identity Finder, then highlight Tools, then highlight and left-click "Secure Microsoft IE Hidden Web Data..."

Once selected, the Secure Microsoft Internet Explorer Hidden Web Data dialog will open. This dialog will have the current Internet Explorer settings for AutoComplete. Disable (uncheck) the ability to save (1) forms and (2) username and passwords.

Next time you use Internet Explorer, it will not save form data for future use. For example, when you are visiting a merchant's website and enter your personal information to make a purchase, Internet Explorer will not save this information. The downside to this is you will need to retype your personal information every time you visit that site, but this is outweighed by the knowledge that no one can access your personal information via Internet Explorer.
Shred Microsoft Internet Explorer (IE) Hidden Web Data Tool

The Shred Microsoft Internet Explorer Locations tool allows you to shred all of the Hidden Web Data stored by Internet Explorer on your computer even if no Identity Match is found there. There are three ways to access the Shred Microsoft IE Hidden Web Data tool:

1. Click the Shred Microsoft IE button on the Tools and Options ribbon.
2. Click the Application Menu button in the upper left corner of Identity Finder, then highlight Tools, then highlight and left-click "Shred Microsoft IE Hidden Web Data..."

Once selected, the Shred Microsoft Internet Explorer Hidden Web Data dialog will open. You can select any or all of the following locations to shred:

- Temporary Internet Files - This includes copies of webpages, images, and media that are saved for faster viewing.
- Cookies - These are files stored on your computer by websites to save preferences such as login information.
- History - This is the list of websites that you have visited.
- Form Data - This is saved information that you have typed into forms.
- Passwords - These are passwords that are automatically filled in when you log on to a website you've previously visited.

Once you have made your selections, click "Shred" and all of your selected locations will be shredded.
Tools to Secure Your Identity

Note: Shredding Internet Explorer Hidden Web Data can take a very long time depending on the amount of information stored on your computer. While shredding is occurring, Identity Finder will display an animation to let you know that it is working.

Note: It is not possible to "undo" a Shred. Shredded results cannot be recovered. Once you shred something, it is gone.
Secure Firefox Hidden Web Data Tool

The Secure Firefox tool allows you to easily configure Firefox to be more secure. When Firefox has saved sensitive passwords and you wish to keep them saved on your computer, you should enable the "Secure Firefox saved passwords with a Master Password" feature. When Firefox has saved sensitive form data and you wish prevent it from doing so in the future, you should disable the "Save information I enter in forms and the Search bar" feature. Firefox Saved Form data cannot be stored securely on your computer. There are two ways to access the Secure Firefox tool:

1. Click the Secure Firefox button on the Tools and Options ribbon.
2. Click the Application Menu button in the upper left corner of Identity Finder, then highlight Tools, then highlight and left-click "Secure Firefox Hidden Web Data..."

Saved Passwords

You can secure Firefox Saved Passwords with a Master Password that encrypts your entire password database. If you do this, all saved passwords will be secured. Simply enter a password and click OK. You may also select the "Securely store this password in your Password Vault". If you click Cancel, no passwords will be secured. After clicking OK, Identity Finder will apply the Master Password. Next time you open Firefox, it will prompt you for the password you entered via Identity Finder before letting you use Saved Passwords. If you forget your password, you will not be able to use Saved Passwords.

Note: Choose a strong password to be sure your data is safe.

Saved Forms

Firefox Saved Form data cannot be stored securely on your computer so you should disable its ability to save form data. Simply disable (uncheck) the ability to save form data to secure Firefox. Next time you use Firefox, it will not save form data for future use. For example, when you are visiting a merchant's website and enter your personal information to make a purchase, Firefox will not save this information. The downside to this is you will need to retype your personal information every time you visit that site, but this is outweighed by the knowledge that no one can access your personal information via Firefox.

Note: This does not remove existing saved form data. Use the Shred Firefox Locations Tool for that.
Shred Firefox Hidden Web Data Tool

The Shred Firefox Locations tool allows you to shred all of the Hidden Web Data stored by Firefox on your computer even if no Identity Match is found there. There are two ways to access the Shred Firefox Locations tool:

1. Click the Shred Firefox button on the Tools and Options ribbon.
2. Click the Application Menu button in the upper left corner of Identity Finder, then highlight Tools, then highlight and left-click "Shred Firefox Hidden Web Data..."

Once selected, the Shred Firefox Hidden Web Data dialog will open. You can select any or all of the following locations to shred:

- **Browsing History** - This is the list of websites that you have visited.
- **Download History** - This is the list of your recently downloaded files.
- **Saved Form and Search History** - This is saved information that you have entered into forms and the Search Bar.
- **Cache** - This includes copies of webpages, images, and media that are saved for faster viewing.
- **Cookies** - These are files stored on your computer by websites to save preferences such as login information and other data.
- **Saved Passwords** - These are passwords that are automatically filled in when you log on to a website you've previously visited.

Once you have made your selections, click "Shred" and all of your selected locations will be shredded.
Note: Shredding Firefox Hidden Web Data can take a very long time depending on the amount of information stored on your computer. While shredding is occurring, Identity Finder will display an animation to let you know that it is working.

Note: It is not possible to "undo" a Shred. Shredded results cannot be recovered. Once you shred something, it is gone.
Licensing, Ordering, and Support

Upgrading from Trial Edition

After you have used the trial edition of Identity Finder and decided to purchase the full version, upgrading is a simple process:

1. Visit http://www.identityfinder.com and purchase a copy of Identity Finder from our secure, online store.
2. Obtain the unique Activation Code provided to you in your email receipt.
3. Launch Identity Finder and select the "Activate Now" option on the Wizard. If you are already within Identity Finder, you may click the "Activate" button on the Main ribbon or on the Application menu.
4. Follow the remaining instructions for Activation.
License Agreement

Identity Finder End User License Agreement

Copyright © 2001-2007 Velosecure, LLC

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF VELOSECURE CAM SOFTWARE ("SOFTWARE") PRODUCED BY VELOSECURE. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT DOWNLOAD OR IF ALREADY HAVE DONE SO, DELETE THE APPLICATION AND REMOVE ALL OF ITS BINARY, DATA, AND OUTPUT FILES FROM YOUR COMPUTER.

1. License Grant. Subject to the payment of the applicable license fees and annual maintenance fees, and subject to the terms and conditions of this Agreement, VELOSECURE ("Velosecure") hereby grants to you a non-exclusive, non-transferable right to use one copy for each seat licensed of the specified version of the Software and the accompanying documentation (the "Documentation"). You may install one copy for each seat licensed of the Software on one computer, workstation, server or other electronic device for which the Software was designed (each, a "Client Device"). You are not permitted to install the Software on any additional computers without first receiving written permission from Velosecure. If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such Software products individually.

- a. Use. The Software is licensed as a single product on the Client Device for which it was purchased; it may not be used on any other Client Device or by more than one user at a time,. The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device.

- b. Server Use. You may use the Software on a Client Device or on or as a server ("Server") within a multi-user or networked environment ("Server Use") only if such use is permitted in the applicable price list or product packaging for the Software. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses you have obtained, then you must have a mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the license you have obtained.

- c. Volume Use. If the Software is licensed with volume license terms specified in the applicable product invoicing or packaging for the Software, you may make, use and install as many additional copies of the Software on the number of Client Devices as the volume license terms specify. You must have a mechanism in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained.

- d. Execution. The Software license allows for its execution on Client Device. VELOSECURE takes no responsibility for the authorization of what constitutes a legal Client Device and it is the onus of the licensee to obtain proper authorization from the Client Device's owner.
2. Term. Velosecure LLC has granted you a perpetual license to use the software. You understand and agree that Velosecure LLC has no obligation to modify the software, provide updates to the software, provide support (except as explicitly stated herein) for the software, assist in installing the software, change the software to run on a different version or release of the operating system, change the software to run on a different operating system, change the software to run on a different platform or make any other changes to the software. This Agreement will terminate automatically if you fail to comply with any of the limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must destroy all copies of the Software and the Documentation.

3. Updates. During the term of this Agreement, you may download revisions, upgrades, or updates to the Software when and as VELOSECURE publishes them via its electronic bulletin board system, website or through other online services upon first transmitting the payment for these items.

4. Ownership Rights. The Software is protected by United States copyright laws and international treaty provisions. VELOSECURE and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except for the use of the software as expressly set forth in this Agreement. All copies of the Software and Documentation made hereunder must contain the same proprietary notices that appear on and in the Software and Documentation.

5. Restrictions. You may not rent, lease, loan or resell the Software. You may not permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement. You may not transfer any of the rights granted to you under this Agreement. You may not reverse engineer, decompile, or disassemble the Software. You may not modify, or create derivative works based upon, the Software in whole or in part. You may not copy the Software or Documentation. You may not remove any proprietary notices or labels on the Software. All rights not expressly set forth hereunder are reserved by Velosecure. Velosecure reserves the right to periodically conduct audits without notice to verify compliance with the terms of this Agreement.

6. Warranty and Disclaimer.
   a. Limited Warranty. VELOSECURE warrants that for one year from the date of original purchase the media (e.g., diskettes) on which the Software is contained will be reasonably free from defects in materials and workmanship.
   b. Customer Remedies. VELOSECURE’s and its suppliers’ entire liability and your exclusive remedy for any breach of the foregoing warranty shall be, at VELOSECURE’s option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media in which the Software is contained. You must return the defective media to VELOSECURE at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent VELOSECURE is subject to restrictions under United States export control laws and regulations.
   c. Warranty Disclaimer. Except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VELOSECURE DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND
NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, VELOSECURE MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

7. Limitation of Liability. UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL VELOSECURE OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES. IN NO EVENT WILL VELOSECURE BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE LIST PRICE VELOSECURE CHARGES FOR A LICENSE TO THE SOFTWARE, EVEN IF VELOSECURE SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU.

8. United States Government. The Software and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

9. Export Controls. Neither the Software nor the Documentation and underlying information or technology may be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods; (ii) to anyone on the United States Treasury Department's list of Specially Designated Nations or the United States Commerce Department's Table of Denial Orders or (iii) to any country or organization prohibited by any agency of the government of the United States. By downloading or using the Software you are agreeing to the foregoing and you are certifying that you are not located in, under the control of, or a national or resident of any such country or on any such list. IN ADDITION, YOU SHOULD BE AWARE OF THE FOLLOWING: EXPORT OF THE SOFTWARE MAY BE SUBJECT TO COMPLIANCE WITH THE RULES AND REGULATIONS PROMULGATED FROM TIME TO TIME BY THE BUREAU OF EXPORT ADMINISTRATION, UNITED STATES DEPARTMENT OF COMMERCE, WHICH RESTRICT THE EXPORT AND RE-EXPORT OF CERTAIN PRODUCTS AND TECHNICAL DATA. IF THE EXPORT OF THE SOFTWARE IS CONTROLLED UNDER SUCH RULES AND REGULATIONS, THEN THE SOFTWARE SHALL NOT BE EXPORTED OR RE-EXPORTED, DIRECTLY OR INDIRECTLY, (A) WITHOUT ALL EXPORT OR RE-EXPORT LICENSES AND UNITED STATES OR OTHER GOVERNMENTAL APPROVALS REQUIRED BY ANY APPLICABLE LAWS, OR (B) IN VIOLATION OF ANY APPLICABLE PROHIBITION AGAINST THE EXPORT OR RE-EXPORT OF ANY PART OF THE SOFTWARE. SOME COUNTRIES HAVE RESTRICTIONS ON THE USE OF ENCRYPTION WITHIN THEIR BORDERS, OR THE IMPORT OR EXPORT OF ENCRYPTION EVEN IF FOR ONLY TEMPORARY PERSONAL OR BUSINESS USE. YOU ACKNOWLEDGE THAT THE IMPLEMENTATION AND ENFORCEMENT OF THESE LAWS IS NOT ALWAYS CONSISTENT AS TO SPECIFIC COUNTRIES. ALTHOUGH THE FOLLOWING COUNTRIES ARE NOT AN EXHAUSTIVE LIST THERE MAY EXIST RESTRICTIONS ON THE EXPORTATION TO, OR IMPORTATION OF, ENCRYPTION BY: BELGIUM, CHINA (INCLUDING HONG KONG), FRANCE, INDIA, INDONESIA, ISRAEL, RUSSIA, SAUDI ARABIA, SINGAPORE, AND SOUTH KOREA. YOU ACKNOWLEDGE IT IS YOUR ULTIMATE RESPONSIBILITY TO COMPLY WITH ANY AND ALL
GOVERNMENT EXPORT AND OTHER APPLICABLE LAWS AND THAT VELOSECURE HAS NO FURTHER
RESPONSIBILITY AFTER THE INITIAL SALE TO YOU WITHIN THE ORIGINAL COUNTRY OF SALE.

10. High-Risk Activities. The Software is not fault-tolerant and is not designed or intended for use in hazardous
environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities,
aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines,
machinery which might cause harm to a person or any other application in which the failure of the Software
could lead directly to death, personal injury, or severe physical or property damage (collectively, "High-Risk
Activities"). VELOSECURE expressly disclaims any express or implied warranty of fitness for High-Risk Activities.

11. Miscellaneous. This Agreement is governed by the laws of the United States and the State of New York,
without reference to conflict of laws principles. The application of the United Nations Convention of Contracts
for the International Sale of Goods is expressly excluded. This Agreement sets forth all rights for the user of the
Software and is the entire agreement between the parties. This Agreement supersedes any other
communications with respect to the Software and Documentation. This Agreement may not be modified except
by a written addendum issued by a duly authorized representative of VELOSECURE. No provision hereof shall be
deemed waived unless such waiver shall be in writing and signed by VELOSECURE or a duly authorized
representative of VELOSECURE. If any provision of this Agreement is held invalid, the remainder of this
Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has
been written in the English language only. VELOSECURE may identify you to the public as a customer of
VELOSECURE and describe in a customer case study the services and solutions delivered by VELOSECURE to you.
VELOSECURE may also issue one or more press releases containing an announcement of the execution and
delivery of this Agreement and/or the implementation of the Software by you. Nothing contained in this Section
11 shall be construed as an obligation by you to disclose any of your proprietary or confidential information to
any third party.

12. VELOSECURE CUSTOMER CONTACT. If you have any questions concerning these terms and conditions, or if
you would like to contact VELOSECURE for any other reason, please use our contact page on our website.
Statements made to you in the course of this sale are subject to the Year 2000 Information and Readiness
Disclosure Act (Public Law 105-271). In the case of a dispute, this Act may reduce your legal rights regarding the
use of any statements regarding Year 2000 readiness, unless otherwise specified in your contract or tariff.

13. This Agreement and all other agreements shall be exclusively construed and interpreted in accordance with
the laws of the State of New York, excluding conflict of laws provisions. No rules, regulations, laws or statutes of
any kind or nature of any other city, county, state or other jurisdiction shall be given any force or effect. You
agree to submit to the personal and the exclusive jurisdiction of the courts (both federal and state) located in
New York County in the State of New York for any action or proceeding brought by you or any other person or
entity. This includes all actions and proceedings of every kind and nature, even if they did not arise out of this
Agreement. Service of a Summons and Complaint upon you by U.S. Mail, Federal Express at the address stated
above or by e-mail shall be the equivalent as if you were personally served with said documents in the State of
New York.

You agree that if you bring any action or proceeding against VELOSECURE you shall do so only in the United
States District Court for the Southern District of New York, unless said court does not have subject matter
jurisdiction, in which case you shall bring any such action or proceeding only in the Supreme Court of the State
of New York, County of New York. The provisions of this paragraph shall apply to all matters and controversies
of every type and nature, including, but not limited to, anything that occurred or pertains to anything prior to
the execution of the Agreement or any other agreement, during the term of the agreement, after the term of
the agreement and for all matters whether or not related to the agreement, the Agreement or any other
agreements. If Velosecure initiates litigation or incur any legal fees as a result of any action that you take or fail
to take or if you breach any term, condition or covenant of this Agreement or any other agreement you shall be responsible for all of Velosecure’s costs, expenses and legal fees of every kind and nature. You agree not to initiate, agree, be part of or in any way participate in any class actions against Velosecure. If you are made a part of a class action you agree to immediately opt out and/or withdraw from being part of the class action. If you do not take corrective action, you agree that you will pay all of your or any other person or entity’s costs, expenses and attorneys fees to do so. You agree not to initiate, agree, be part of or in any way participate in any with any other person, business or entity against Velosecure as a plaintiff or in any other capacity in any lawsuit, complaint to any agency or in any other proceeding. If you violate the terms of the previous sentence you agree to immediately take corrective action to come into compliance with those terms. If you do not take immediately corrective action, you agree that you will pay all of you or any other person or entity’s costs, expenses and attorneys fees to do so. There may be state laws which conflict with these provisions, in which instance such state law shall prevail.

YOU HEREBY AGREE TO WAIVE ALL RIGHTS OF EVERY KIND AND NATURE FOR TRIAL BY JURY FOR ALL CLAIMS, COUNTERCLAIMS, CROSS-CLAIMS AND FOR ALL OTHER ACTIONS, CASES AND PROCEEDINGS. IT IS AGREED AND UNDERSTOOD THAT UNDER NO CIRCUMSTANCES WILL ANY CASE BE TRIED BEFORE A JURY FOR ANY REASON WHATSOEVER.

Notwithstanding anything to the contrary herein, all provisions hereof are hereby limited to the extent mandated by any applicable law, regulation or decision. If any one or more paragraphs, clauses or other portions hereof should ever be determined to be illegal, invalid or otherwise unenforceable by a court of competent jurisdiction, or to be illegal, invalid or invalidated or unenforceable by reason of any existing or later enacted law, regulation or statute, then to the extent it is within the jurisdiction illegal, invalid or unenforceable, it shall be limited or construed so as to be valid and enforceable or severed and deleted herefrom. The remaining portions hereof shall survive, remain in full force and effect, continue to be binding and shall not be affected except insofar as may be necessary to make sense hereof, and shall be interpreted to give effect to the intention of the parties insofar as that is possible.

The rights and remedies of Velosecure provided in this Agreement shall be in addition to (and not in substitution for) any and all rights and remedies to which Velosecure shall be entitled at law or equity. The covenants contained in this Agreement shall be construed as separate and independent of any other provision of this Agreement.
Contacting Velosecure for Support

If you need support or have a question you can always E-Mail us. Additionally, the Velosecure and Identity Finder team is extremely grateful to our large customer base for all their feedback. Whether you have an improvement you would like us to make or want to share your experience, we always read and respond to your E-Mails in a timely manner.

Please send all feedback to:

support@identityfinder.com
Submitting Feedback to Identity Finder Team

If you need support or have a question you can always e-mail us. Additionally, the Velosecure and Identity Finder teams are extremely grateful to our large customer base for all their feedback. Whether you have an improvement you would like us to make or want to share your experience, we always read and respond to your E-Mails in a timely manner.

Please send all feedback to:

support@identityfinder.com
Hints and Tips

What Information is Sent over Internet to Identity Finder Servers

When you run Identity Finder for the first time and activate the software, your activation code is sent to Velosecure's Identity Finder server. This only occurs during activation. During registration, if you choose to enter your e-mail address, name, and other contact information, it will be sent once during that process. We do not collect personal information found by the software. During Check for Updates, which is enabled by default, the version of Identity Finder you are running is sent to the server.
How Frequently Should You Search Your Data

It is extremely important to run Identity Finder weekly to protect your identity, as during each week you are accessing the internet, receiving E-Mails, and modifying files. You can schedule Identity Finder to run on a periodic basis via the Results Wizard, the Scheduling button, or the Settings dialog box.
What Encryption Does Identity Finder Use

This topic addresses how Identity Finder securely saves your results in the *.idf proprietary format and how Identity Finder securely saves your personal list of identities for the include list (as well as ignored identities and locations).

Identity Finder uses AES 256 bit encryption that is FIPS 140-2 validated. Cert #119. More information can be found on the National Institute of Standards and Technology's Cryptographic Module Validation Program page: http://csrc.nist.gov/cryptval/140-1/1401val2007.htm
What is FIPS 140-2

FIPS stands for the Federal Information Processing Standards. The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235). Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235). The 140-2 standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information).

Identity Finder uses AES 256 bit encryption that is FIPS 140-2 validated. Cert #119. More information can be found on the National Institute of Standards and Technology's Cryptographic Module Validation Program page: http://csrc.nist.gov/cryptval/140-1/1401val2007.htm
What are Secure Items Skipped?

When you enable logging, you have the ability to log Secure Items Skipped. Secure Items Skipped are locations on your computer that Identity Finder did not search because they were already secured with encryption.
Choosing Strong Passwords

Identity Finder provides you the ability to enforce good behavior and pick strong passwords. The guidance below is helpful for choosing strong passwords:

A strong password is easy for you to remember but hard for someone else to guess and contains a mix of at least uppercase letters, lowercase letters, and digits. Even stronger passwords may contain a symbol. A password of six characters is sufficient, shorter passwords are easier to guess and longer passwords are great as long as they are not too difficult for you to remember without writing it down.

Strong passwords:
- Have upper or lower case letters.
- Have digits and/or punctuation characters.
- Are six characters long.
- Are easy for you to remember, so you will not be tempted to write them down.
- Can be typed quickly, so someone else cannot look over your shoulder and learn it.

Stronger passwords:
- Have both upper and lower case letters.
- Have digits and/or punctuation characters.
- Are eight characters long.
- Are easy for you to remember, so you will not be tempted to write them down.
- Can be typed quickly, so someone else cannot look over your shoulder and learn it.

A strong password is not:
- Personal information such as your name, phone number, social security number, birth date or address.
- Any word in the dictionary - in any language, or based closely on such a word (such as a word spelled backwards).
- A word with letters simply replaced by digits. For example, P@ssw0rd is not a strong password.
- A sequence or repeated characters. "12345678," "222222," "abcdefg," or adjacent letters on your keyboard.
Installing Additional Filters

Identity Finder can already search more than 200 of the most common file types using its built-in filters and a built-in feature of Microsoft Windows available since Windows 2000 called IFilters. For these filterable file types, Identity Finder can search the file while preserving the format and structure of the file. Additionally, Identity Finder can attempt to extract text from any file. As new, proprietary file types are created that Identity Finder cannot search while preserving format and structure, additional IFilters may be created to search them. Using an IFilter rather than relying on Identity Finder to extract the text from a file will increase the ability to find true positives and reduce false positives. This is the case because Identity Finder uses the context and structure of files to look for specific types of information and determine if a potential match is truly personal information. If you install any of these additional IFilters, Identity Finder will automatically detect and utilize them for all of your future searches.

If the filter for a file type you want to search is not already built into Identity Finder, you may be able to download and install an appropriate IFilter. To learn more about IFilters or to download one, visit Microsoft's IFilter website. For even more information, you can also visit Channel 9 discussion on Search IFilters, or visit IFilter.org.

To enable searching of Office 2007 files, Microsoft OneNote files, and/or Microsoft Visio files without having to install those applications, you may download and install Microsoft's Filter Pack for free. It is available here: http://www.microsoft.com/downloads/details.aspx?FamilyId=60C92A37-719C-4077-B5C6-CAC34F4227CC&displaylang=en
Using the System Tray Icon

The system tray icon allow quick access to common tasks:

- **Minimize/Maximize to Tray**
  - Show Status Window
  - Show Tray Popups
  - Hide Tray Icon

- Password Vault
- Settings
- Exit

One additional feature on the System Tray Icon is "Minimize/Maximize to Tray", which allows you to hide the entire Identity Finder application and remove it from the task bar in Windows. This is helpful if you are running Identity Finder and you know it will not finish soon but do not want it in your way.
Benefits

Quickly search your files, E-Mails, and system areas:
Identity Finder uses proprietary search algorithms to uncover multiple variations of specific types of personally identifiable information such as social security numbers and credit card numbers. Areas searched include your web browser’s hidden storage areas such as auto complete fields (i.e., passwords and form data); web pages and cookies; instant messenger logs; home and office files; compressed files; E-Mails and attachments; the Windows registry, and more.

Locate your personally identifiable information:
Identity Finder has been specifically designed to locate personal information without requiring you to enter this information yourself. This feature allows the software to search your computer for any personally identifiable information &endash; including that of your family, friends and colleagues or any home or business user. Information uncovered by Identity Finder includes social security numbers, individual taxpayer numbers, employer information numbers, credit and debit card numbers, driver’s license and other state-issued identification numbers, military identification numbers, dates of birth and personal addresses, telephone numbers, bank account numbers, passwords and PINs, employee identification numbers, and mother’s maiden names.

Securely delete or encrypt your sensitive information:
One of the most common ways of leaving personal information exposed to compromise is by assuming that deleting a file or data digitally erases it. It doesn’t. “Deleted” files are first stored in your Recycle Bin where they can be easily read by any person or program with access to your computer. Even when Recycle Bin is emptied, file remnants remain &endash; and can be easily un-“deleted” with common tools. When this, or any other personal information, is uncovered you are presented with several choices. Identity Finder can encrypt the file, so that a password is needed to access and read it and you don’t need to destroy the information to protect it. Or it will securely erase the data and remove it from your computer once and for all.
Configuration Settings Files for Scheduling Tasks

Configuration Settings files are configuration settings to be used when you want to schedule a task and force parameters to override any user settings on that machine. You may use the Settings dialog to export this file or manually create it yourself. None of the entries are required except for the header (indicated as the first row in the table below).

The following settings can be exported from the Settings dialog:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options and Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[JobSettings]</td>
<td>Required header</td>
</tr>
<tr>
<td>AnyFind_doBankAccount</td>
<td>0 or 1: Specifies whether to enable the searching of Bank Accounts using AnyFind</td>
</tr>
<tr>
<td>AnyFind_doCCN</td>
<td>0 or 1: Specifies whether to enable the searching of Credit Cards using AnyFind</td>
</tr>
<tr>
<td>AnyFind_doPassword</td>
<td>0 or 1: Specifies whether to enable the searching of Passwords using AnyFind</td>
</tr>
<tr>
<td>AnyFind_doSSN</td>
<td>0 or 1: Specifies whether to enable the searching of Social Security Numbers using AnyFind</td>
</tr>
<tr>
<td>createOutputFolder</td>
<td>0 or 1: Specifies whether to create the output folder for your saved file, if one does not exist.</td>
</tr>
<tr>
<td>createOutputFolder2</td>
<td>0 or 1: Specifies whether to create the secondary output folder for your saved file, if one does not exist.</td>
</tr>
<tr>
<td>customFolderExcludeList</td>
<td>Full Folder Paths to folders you want Identity Finder to exclude from the search, if you selected the Custom Folder Option (see folderOpt option 2 below). Separate multiple paths with the pipe (</td>
</tr>
<tr>
<td>customFolderList</td>
<td>Full Folder Paths to folders you want Identity Finder to search, if you selected the Custom Folder Option (see folderOpt option 2 below). Separate multiple paths with the pipe (</td>
</tr>
<tr>
<td>doAttachments</td>
<td>0 or 1: Specifies whether to enable the searching of E-Mail Attachments</td>
</tr>
<tr>
<td>doCompressed</td>
<td>0 or 1: Specifies whether to enable the searching of Compressed Files</td>
</tr>
<tr>
<td>doDocuments</td>
<td>0 or 1: Specifies whether to enable the searching of Files (uncompressed)</td>
</tr>
<tr>
<td>doHWD</td>
<td>0 or 1: Specifies whether to enable the searching of Hidden Web Data</td>
</tr>
<tr>
<td>doMessages</td>
<td>0 or 1: Specifies whether to enable the searching of E-Mail Messages</td>
</tr>
<tr>
<td>doRegistry</td>
<td>0 or 1: Specifies whether to enable the searching of the Windows Registry</td>
</tr>
<tr>
<td>exitOnComplete</td>
<td>0 or 1: Specifies whether to automatically exit Identity Finder when the search completes.</td>
</tr>
<tr>
<td>extensionSearchMode</td>
<td>0 or 1 or 2 or 3: Specifies whether to search only common files, all filterable file types, a custom file type list, or all files.</td>
</tr>
<tr>
<td>folderOpt</td>
<td>0 or 1 or 2: Specifies whether to search for files inside My Documents (0), My Computer (1), or Custom (2). If you choose Custom, see customFolderList above.</td>
</tr>
<tr>
<td>runLowPriority</td>
<td>0 or 1: Specified whether to give other applications priority over Identity Finder.</td>
</tr>
<tr>
<td>saveFolderLoc</td>
<td>Full path and file name for the saved results. The results will be saved with the encrypted password from saveKey.</td>
</tr>
<tr>
<td>saveFolderLoc2</td>
<td>Full path and file name for the secondary saved results. The results will</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>saveKey</td>
<td>Encrypted password to save your results. You must use the main program to produce this key.</td>
</tr>
<tr>
<td>saveKey2</td>
<td>Encrypted password to save your secondary results. You must use the main program to produce this key (used with saveFolderLoc2).</td>
</tr>
<tr>
<td>saveToFile</td>
<td>0 or 1: Specifies whether to save the Identity Finder results to a file automatically. You must specify a saveFolderLoc and saveKey for this feature to work correctly.</td>
</tr>
<tr>
<td>saveToFile2</td>
<td>0 or 1: Specifies whether to save the Identity Finder results to a secondary file automatically. You must specify a saveFolderLoc and saveKey2 for this feature to work correctly.</td>
</tr>
<tr>
<td>useEmailMTime</td>
<td>0 or 1: Specifies whether to search only E-mails created or modified since the last search run using this option.</td>
</tr>
<tr>
<td>useEmailUTime</td>
<td>0 or 1: Specifies whether to search only E-mails created or modified since a specified date (see also EmailUTimeDateUINITlow and EmailUTimeDateUINIThigh).</td>
</tr>
<tr>
<td>useFileUTime</td>
<td>0 or 1: Specifies whether to search only files created or modified since a specified date (see also FileUTimeDateUINITlow and FileUTimeDateUINIThigh).</td>
</tr>
<tr>
<td>EmailUTimeDateUINITlow</td>
<td>An unsigned integer representing the low order part of a FILETIME value to be used with useEmailUTime.</td>
</tr>
<tr>
<td>EmailUTimeDateUINIThigh</td>
<td>An unsigned integer representing the high order part of a FILETIME value to be used with useEmailUTime.</td>
</tr>
<tr>
<td>FileUTimeDateUINITlow</td>
<td>An unsigned integer representing the low order part of a FILETIME value to be used with useFileUTime.</td>
</tr>
<tr>
<td>FileUTimeDateUINIThigh</td>
<td>An unsigned integer representing the high order part of a FILETIME value to be used with useFileUTime.</td>
</tr>
<tr>
<td>Logging_enable</td>
<td>0 or 1: Specifies whether to enable logging for the search.</td>
</tr>
<tr>
<td>Logging_logpath</td>
<td>Full path to the folder where the log files should be saved.</td>
</tr>
<tr>
<td>Logging_retention</td>
<td>0 or 1: Specifies whether to (1) create a new log file for each search session or to (2) append new information to the previous log file.</td>
</tr>
<tr>
<td>Logging_format</td>
<td>0 or 1 or 2: Specifies the format to save the log file as. (1) Tab separated values, (2) Comma separated values, or (3) Fixed width format.</td>
</tr>
<tr>
<td>Logging_encryption</td>
<td>0 or 1: Specifies whether to enable encryption of the log file.</td>
</tr>
<tr>
<td>Logging_doItemsSearched</td>
<td>0 or 1: Specifies whether to enable the logging of the location of all items searched.</td>
</tr>
<tr>
<td>Logging_doMatchingItems</td>
<td>0 or 1: Specifies whether to enable the logging of the location of all matching items.</td>
</tr>
<tr>
<td>Logging_doSecureItemsSkipped</td>
<td>0 or 1: Specifies whether to enable the logging of the location of all secure items skipped.</td>
</tr>
<tr>
<td>Logging_doMessages</td>
<td>0 or 1: Specifies whether to enable the logging of the location of all messages.</td>
</tr>
<tr>
<td>Logging_doUserActions</td>
<td>0 or 1: Specifies whether to enable the logging of the location of all user actions.</td>
</tr>
<tr>
<td>Logging_doErrors</td>
<td>0 or 1: Specifies whether to enable the logging of the location of all errors.</td>
</tr>
</tbody>
</table>
If you want to set any of the following options, they must be added to the file manually:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options and Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyFind_enable_AU_TFN</td>
<td>0 or 1: Specifies whether to enable the ability to search for Australian Tax File Numbers. This option does not turn on this searching, for that, refer to doAU_TFN.</td>
</tr>
<tr>
<td>AnyFind_enable_Canada_SIN</td>
<td>0 or 1: Specifies whether to enable the ability to search for Canadian Social Insurance Numbers. This option does not turn on this searching, for that, refer to doCanada_SIN.</td>
</tr>
<tr>
<td>AnyFind_enable_UK_NINO</td>
<td>0 or 1: Specifies whether to enable the ability to search for United Kingdom National Insurance Numbers. This option does not turn on this searching, for that, refer to doUK_NINO.</td>
</tr>
<tr>
<td>AnyFind_enable_UK_NHS</td>
<td>0 or 1: Specifies whether to enable the ability to search for United Kingdom National Health Service Numbers. This option does not turn on this searching, for that, refer to doUK_NHS.</td>
</tr>
<tr>
<td>AnyFind_doAU_TFN</td>
<td>0 or 1: Specifies whether to enable the searching of Australian Tax File Numbers using AnyFind (must also set enable_AU_TFN to 1).</td>
</tr>
<tr>
<td>AnyFind_doCanada_SIN</td>
<td>0 or 1: Specifies whether to enable the searching of Canadian Social Insurance Numbers using AnyFind (must also set enable_Canada_SIN to 1).</td>
</tr>
<tr>
<td>AnyFind_doUK_NINO</td>
<td>0 or 1: Specifies whether to enable the searching of United Kingdom National Insurance Numbers using AnyFind (must also set enable_UK_NINO to 1).</td>
</tr>
<tr>
<td>AnyFind_doUK_NHS</td>
<td>0 or 1: Specifies whether to enable the searching of United Kingdom National Health Service Numbers using AnyFind (must also set enable_UK_NHS to 1).</td>
</tr>
<tr>
<td>useMaxFileSize</td>
<td>0 or 1: Specifies whether to only search files larger than the specified max file size (see also MaxFileSize)</td>
</tr>
<tr>
<td>MaxFileSize</td>
<td>Size in MB of the largest file that should be searched (must also set useMaxFileSize to 1)</td>
</tr>
<tr>
<td>doExchangeMailServerFolders</td>
<td>0 or 1: Specifies whether to search Exchange mail server folders as part of the E-Mail message search.</td>
</tr>
<tr>
<td>includeOutlookInEmailSearch</td>
<td>0 or 1: Specifies whether to search Microsoft Outlook as part of the E-Mail message search.</td>
</tr>
<tr>
<td>includeWinmailInEmailSearch</td>
<td>0 or 1: Specifies whether to search Microsoft Outlook Express or Windows Vista Mail as part of the E-Mail message search.</td>
</tr>
<tr>
<td>includeIEInHWDSearch</td>
<td>0 or 1: Specifies whether to search Microsoft Internet Explorer as part of the Hidden Web Data search.</td>
</tr>
<tr>
<td>includeFFOXInHWDSearch</td>
<td>0 or 1: Specifies whether to search Firefox as part of the Hidden Web Data search (see also includeFFOXInHWDSearch_Passwords and includeFFOXInHWDSearch_FormData)</td>
</tr>
<tr>
<td>includeFFOXInHWDSearch_Passwords</td>
<td>0 or 1: Specifies whether to search Firefox Passwords as part of the Hidden Web Data search (must also set includeFFOXInHWDSearch to 1)</td>
</tr>
<tr>
<td>includeFFOXInHWDSearch_FormData</td>
<td>0 or 1: Specifies whether to search Firefox Form Data as part of the Hidden Web Data search (must also set includeFFOXInHWDSearch to 1)</td>
</tr>
<tr>
<td>searchComputerforHWDPasswords</td>
<td>0 or 1: Specifies whether to search all other locations for</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>doRestrictResults</td>
<td>0 or 1: Specifies whether to restrict the number of identity matches displayed per locations (see also doRestrictResults_setting_x and doRestrictResults_setting_y).</td>
</tr>
<tr>
<td>doRestrictResults_setting_x</td>
<td>The threshold for the number of matches in a location above which the number of results should be restricted (must also set doRestrictResults to 1 and doRestrictResults_setting_y to the desired amount).</td>
</tr>
<tr>
<td>doRestrictResults_setting_y</td>
<td>The number of results to display in each location that has more identity matches than the specified threshold (must also set doRestrictResults to 1 and doRestrictResults_setting_x to the threshold amount).</td>
</tr>
<tr>
<td>useRegexForUserDefinedType</td>
<td>0 or 1: Specifies whether to treat the entries added to the include list as &quot;User Defined Types&quot; as (1) regular expressions or (0) as literal strings.</td>
</tr>
<tr>
<td>doQuarantineLeaveFileBehind</td>
<td>0 or 1: Specifies whether to leave a text file in the place of each quarantined file noting the new location of the quarantined file.</td>
</tr>
<tr>
<td>quarantineFolderLoc</td>
<td>Full path to the default location to be selected for the Quarantine location.</td>
</tr>
</tbody>
</table>

**Sample .ini file:**

```
[JobSettings]
AnyFind_doBankAccount=1
AnyFind_doCCN=1
AnyFind_doPassword=1
AnyFind_doSSN=1
createOutputFolder=1
customFolderList=c:\;d:\
doAttachments=1
doCompressed=1
doDocuments=1
doHWD=1
doMessages=1
doRegistry=1
exitOnComplete=1
folderOpt=2
saveFolderLoc=c:\results.idf
saveKey=fd66fc7d21db6c67542b562657b1d9983066cb353be8d974cb90afa9b632e5c08926bd91d4d806fbaee28a363e0822430305f6309e5b723b
saveToFile=1
```

**Scheduling a Task Using Your Configuration Settings File**

To schedule Identity Finder to run with your Configuration Settings file setting, schedule the following task to run:

```
identityfinder.exe /jobmode /inifile="c:\full path to\filename.ini"
```
Shredder Technology

The shredder technology is based on the United States Department of Defense Directive 5220.22-M, which provides baseline standards for the protection of classified information. It uses multiple levels of deletion so that the file you delete may not be recovered, even by undelete programs. You can read more on the Defense Technical Information Center website: [http://www.dtic.mil/whs/directives/corres/html/522022m.htm](http://www.dtic.mil/whs/directives/corres/html/522022m.htm)
Troubleshooting

Identity Finder is Not Working Properly

If Identity Finder is encounters an error that it cannot recover from, you will probably see this error message:

Message: Identity Finder has encountered a problem and needs to close. We apologize for the inconvenience.

Reason: There was an error that caused Identity Finder to terminate.

Screenshot:

<table>
<thead>
<tr>
<th>Identity Finder Home Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Finder has encountered a problem and needs to close. We apologize for the inconvenience.</td>
</tr>
</tbody>
</table>

To help us resolve this issue, we have collected information about the current state of Identity Finder and would appreciate the following assistance:

Step 1: Click the "Save" button to save this report on your computer
Step 2: Send an e-mail, with the saved report as an attachment, to support@identityfinder.com
Step 3: Click the "Close" button to dismiss this window

Thank you for your patience and we will reply to you with an update as soon as possible.

Solution:
When this happens, Identity Finder collects some information to help the support team determine the cause of the issue and correct it. A zip file is automatically created that contains up to 3 files:

- errorlog.log - This file contains information about the version and edition of Identity Finder you were running, some non-personal information about your computer such as your operating system and memory status, and some information about the other applications running on your computer. This file is in clear text.
- identityfinder.dmp - This file contains specific information about what Identity Finder was doing at the moment of the error. Our support engineers can use the information in this file to help them correct the issue.
- screenshot.bmp - This file is an image of Identity Finder just before the error occurred. This can often assist our engineers in determining the cause of the issue. Because this screenshot may contain your personal information, you may delete this file before sending us the error report.

As noted in the window above, please click the "Save" button and choose a location to save the error report Zip file on your computer. If you would like to delete the screenshot before sending the report, open the zip file and remove that file screenshot.bmp. Once the report file is saved, please compose and e-mail to support@identityfinder.com (or click the link in the window above to open your default mail program) and attach the saved report file.

If you would like to see the files that will be sent without having to open the saved Zip file manually, you can click the Preview button to open the window below. Once open, you can click on any of the 3 files to see a preview. The identityfinder.dmp file will most likely contain information that is not human-readable.
Contacting Technical Support

You may contact technical support at any time to ask questions or provide comments. If Identity Finder did not complete successfully, please email as much information about your search as possible and send your dmp report, if there is one in your Identity Finder folder. It does not contain any personal information. Contact technical support by emailing:

support@identityfinder.com
Warning Messages

This page serves to provide descriptions to warning messages you might encounter while using Identity Finder. Many of these messages are simply information and do not indicate a problem.

---

**Message:** This file no longer exists. Would you like to remove this row from the results view.

**Reason:** This might occur when a file has already been removed from your system by another process. Perhaps the file was a temporary file being used by another program and was already deleted.

**Screenshot:**

---

**Message:** This application has failed to start because IdentityFinder.dll was not found. Re-installing the application may fix this problem.

**Reason:** The file IdentityFinder.dll is required to be in the same folder as IdentityFinder.exe. You must reinstall Identity Finder.

**Screenshot:**

---

**Message:** The file you have selected is not a saved results file. Please select another file and try again.
**Reason:** You attempted to load a file into Identity Finder that is not a *.idf file format.

**Screenshot:**

![Identity Finder Open Results Error](image)

**Message:** Identity Finder was unable to open your saved results file.

**Reason:** The folder to which you installed Identity Finder is write protected or you do not have permission to write to it. Check the security permissions of the folder and ensure you are allowed full control of the folder and its contents.

**Screenshot:**

![Identity Finder Open Results Error](image)

**Message:** Your installation of Identity Finder is corrupt. Please download and re-install the newest version of the software from http://www.identityfinder.com. If you have any questions or concerns, please E-Mail identityfinder.com.

**Reason:** One of the supporting files that Identity Finder installs and requires for execution is missing or has been modified.

**Screenshot:**
Identity Finder

Identity Finder

Your installation of Identity Finder is corrupt. Please download and re-install the newest version of the software from http://www.identityfinder.com. If you have any questions or concerns, please contact support@identityfinder.com.
Glossary

E

Encrypt: Secure your data so that it can no longer be read without first inputting a password.

S

Secure Items Skipped: Locations on your computer that Identity Finder did not search because they were already secured with encryption.

Shred: Permanently delete your data. For files this using a standard implemented by the U.S. Department of Defense. For other data it permanetly removes it from your hard drive.