University of Connecticut

Information Security Office

Identity Finder
User Guide

Author: Information Security Office
Date Last Revised: 01/18/2012

identityfinder

Table of Contents

University of Connecticut
Information Security Office

identityfinder

Quick Start Guide

UConn & You - Working Together to Protect Personal Information

What Is Identity Finder?

Identity Finder is software that gives you the ability to find and protect sensitive data on computers, helping to prevent data loss and identity theft. We refer to this data as PII - Personally Identifiable Information.

Why Are We Using Identity Finder?

UConn is using Identity Finder to proactively locate PII in order to protect its students, faculty, staff and affiliates.

How Do I Install It On My Computer?

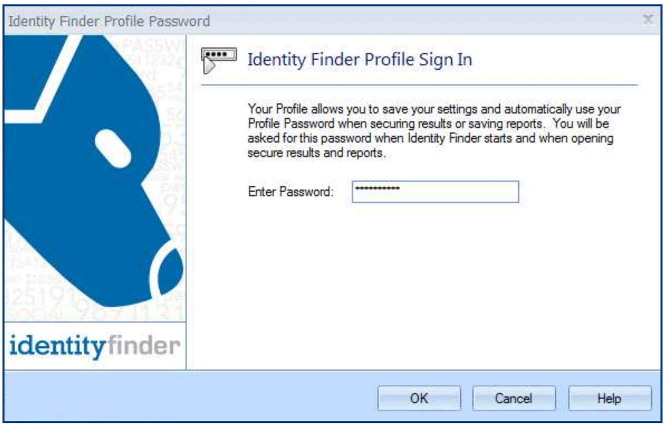
NetID & password are to access the files.

- Identity Finder for Windows can be downloaded here: https://web2.uconn.edu/idfinder/download/IDFinder_Windows_v5.6.msi
- Identity Finder for Macintosh can be downloaded here: https://web2.uconn.edu/idfinder/download/IDFinder_Mac_v5.6.pkg.zip

Step 1: Log On

1

During the install process of the Identity Finder application, users were asked to select and enter a password that would be used to log into the application.
After selecting the Identity Finder icon from the desktop, users will be asked to enter the password on the 'Profile Sign In' pop-up box that they selected during the install process.
After entering the password, click "**OK**".



Identity Finder Profile Password

Identity Finder Profile Sign In

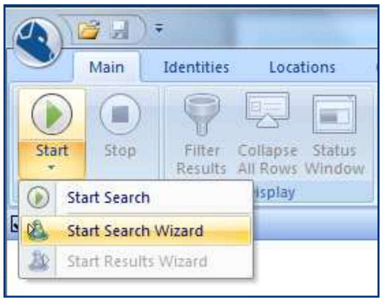
Your Profile allows you to save your settings and automatically use your Profile Password when securing results or saving reports. You will be asked for this password when Identity Finder starts and when opening secure results and reports.

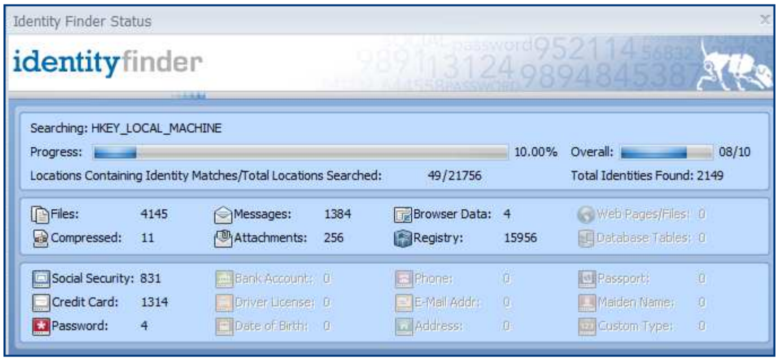
Enter Password: ************

Step 2: Search Out the PII

2

1. Click on the "**Start**" option from the main toolbar.
2. Select either:
   - "**Start Search**" which will do a general search for files that contain Social Security and Credit Card PII.
   - "**Start Search Wizard**" allows for a nonspecific method of searching called "*AnyFind*". *AnyFind* will return any file that contains a piece of PII. This type is the preferred method for discovering all PII that may exist on the user's computer.
3. Once the search begins, the 'Identity Finder Status' box will be displayed.





Identity Finder Status

Searching: HKEY_LOCAL_MACHINE

Progress: 10.00% Overall: 08/10

Locations Containing Identity Matches/Total Locations Searched: 49/21756 Total Identities Found: 2149

Files:	4145	Messages:	1384	Browser Data:	4	Web Pages/Files:	0
Compressed:	11	Attachments:	256	Registry:	15956	Database Tables:	0
Social Security:	831	Bank Account:	0	Phone:	0	Passport:	0
Credit Card:	1314	Driver License:	0	E-Mail Addr:	0	Maiden Name:	0
Password:	4	Date of Birth:	0	Address:	0	Custom Type:	0

Step 3: Evaluate and “Handle” the Results 3

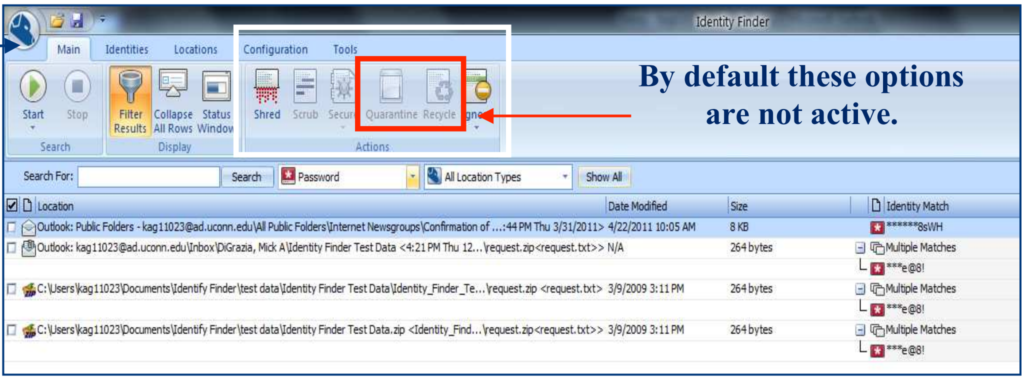
After the files containing PII are located, the users must then determine what to do with it.

1. Select the file (s) to “handle”.
2. Select one of the following options from the ‘Main’ application toolbar:
   - **Shred** - this option should be used when the file found is no longer needed on the user’s computer. Any file shredded **can not** be recovered.
   - **Scrub** - this option should be used when the file found is still needed but the PII part of the file is not.

     The Scrub option can only be performed on certain types of files specifically plain text and non-proprietary file types. Email messages, attachments, PDF files, and files within .zip files cannot be scrubbed. Additionally, the Scrub option will not function on computers running Microsoft Office 2003 or earlier.
   - **Ignore** - this option should be utilized when a false positive result is found.

Note: The options Recycle, Quarantine and Secure are currently not available.

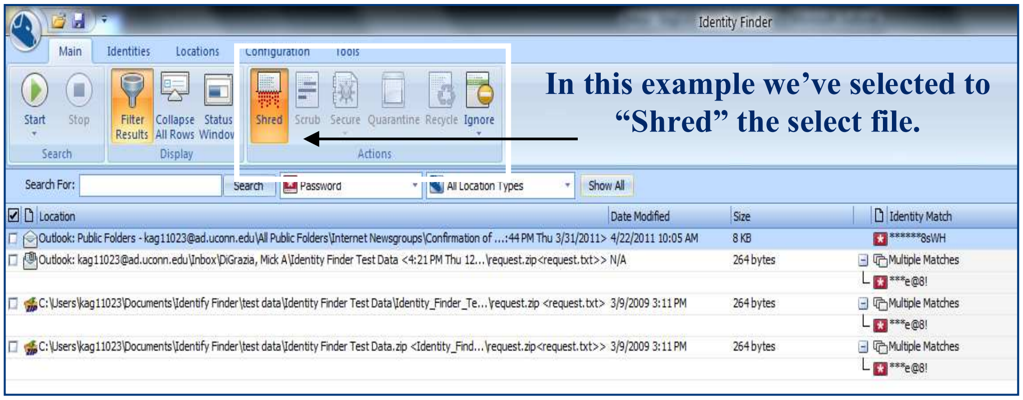
3. Confirm or deny the action selected by either clicking “**Yes**” or “**No**”.
4. Once the action is complete, the user will be shown a confirmation message.
5. Click “**OK**”.



By default these options are not active.

Search For: Search Password All Location Types Show All

☑	Location	Date Modified	Size	Identity Match
□	Outlook: Public Folders - kag11023@ad.uconn.edu\All Public Folders\Internet Newsgroups\Confirmation of ...:44 PM Thu 3/31/2011>	4/22/2011 10:05 AM	8 KB	******8sWH
□	Outlook: kag11023@ad.uconn.edu\Inbox\DiGrazia, Mick A\Identity Finder Test Data <4:21 PM Thu 12...\request.zip<request.txt>>	N/A	264 bytes	Multiple Matches ***e@8!
□	C:\Users\kag11023\Documents\Identify Finder\test data\Identity Finder Test Data\Identity_Finder_Te...\request.zip <request.txt>	3/9/2009 3:11 PM	264 bytes	Multiple Matches ***e@8!
□	C:\Users\kag11023\Documents\Identify Finder\test data\Identity Finder Test Data.zip <Identity_Find...\request.zip<request.txt>>	3/9/2009 3:11 PM	264 bytes	Multiple Matches ***e@8!



In this example we’ve selected to “Shred” the select file.

Search For: Search Password All Location Types Show All

☑	Location	Date Modified	Size	Identity Match
□	Outlook: Public Folders - kag11023@ad.uconn.edu\All Public Folders\Internet Newsgroups\Confirmation of ...:44 PM Thu 3/31/2011>	4/22/2011 10:05 AM	8 KB	******8sWH
□	Outlook: kag11023@ad.uconn.edu\Inbox\DiGrazia, Mick A\Identity Finder Test Data <4:21 PM Thu 12...\request.zip<request.txt>>	N/A	264 bytes	Multiple Matches ***e@8!
□	C:\Users\kag11023\Documents\Identify Finder\test data\Identity Finder Test Data\Identity_Finder_Te...\request.zip <request.txt>	3/9/2009 3:11 PM	264 bytes	Multiple Matches ***e@8!
□	C:\Users\kag11023\Documents\Identify Finder\test data\Identity Finder Test Data.zip <Identity_Find...\request.zip<request.txt>>	3/9/2009 3:11 PM	264 bytes	Multiple Matches ***e@8!

Option to “Save” Results:

To Save Search Results to Manage at a Later Time:

1. 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).
2. You have the option to save the entire result file or only select records. To save select rows, select the checkbox to the left of the result record.
3. Click “**Save**” and select the folder location and filename for your results.
4. 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.

Step 4: Log Out

For **help and support** with Identity Finder contact the UITS Help Center:
E-Mail: helpcenter@uconn.edu
Phone: 860-486-4357

User Manual

What is PII (Personal Identifiable Information)?

PII is a blanket term covering any form of data used to uniquely identify a person. Some examples of this form of data are listed below:

- Credit Card Numbers
- Social Security Numbers
- Bank Account Numbers
- Passwords
- Passports and Drivers Licenses Numbers

Like any other form of data, PII that is stored on your computer can be neglected or misplaced over time. However, PII differs in the sense that if your machine becomes compromised this data can facilitate identity theft.

How is UConn Protecting Us?

The University has recognized this threat and is taking proactive measures to protect its students, faculty, staff and affiliates by implementing software to locate, protect or dispose PII data.

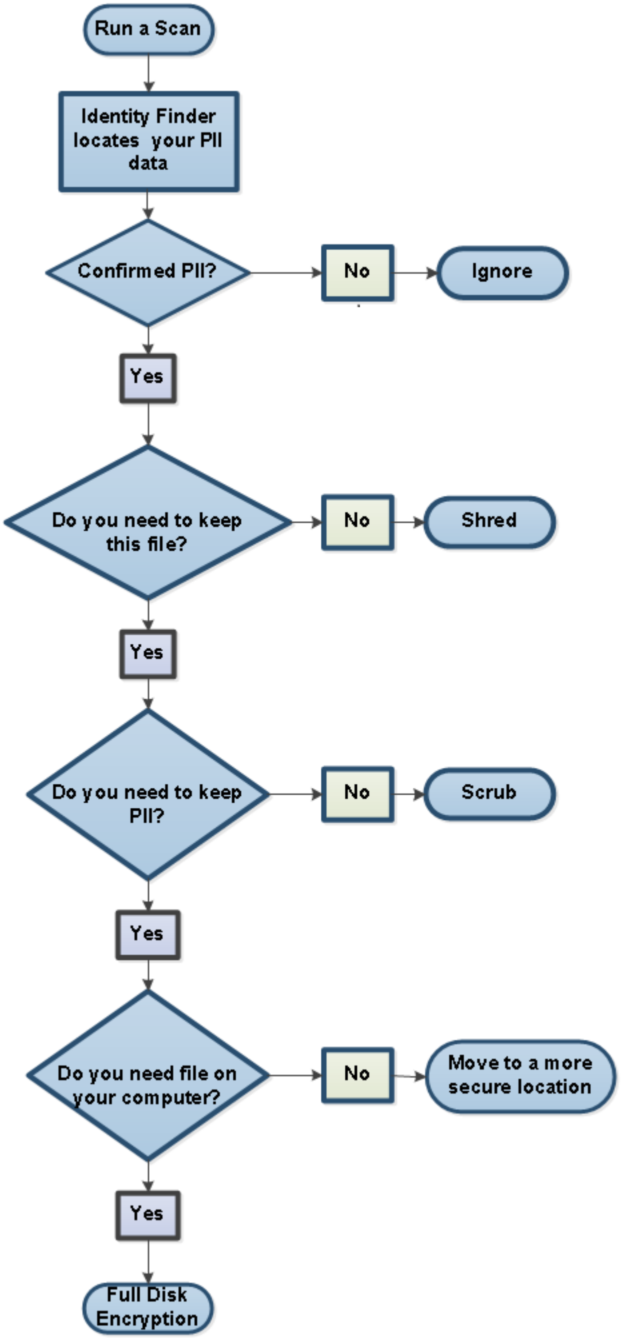
Identity Finder licenses have been purchased by the University and can be used by any faculty and staff on University-owned computers.

Users can download Identity Finder from the following website: http://identityfinder.uconn.edu. Once installed, users may scan their local machines at their convenience.

How Does It Work?

Identity Finder works by searching your computer for *patterns;* for example, if you run a search looking for social security numbers Identity Finder will go through any pattern matching the **XXX-XX-XXXX** social security structure. Scans are extremely easy to initiate and customize. Identity Finder will consume some system resources while a scan it in progress, however, it will be possible to maintain productivity while it is running. Subsequent scans will not consume as much system resources.

What Do I Do With the Data Found?

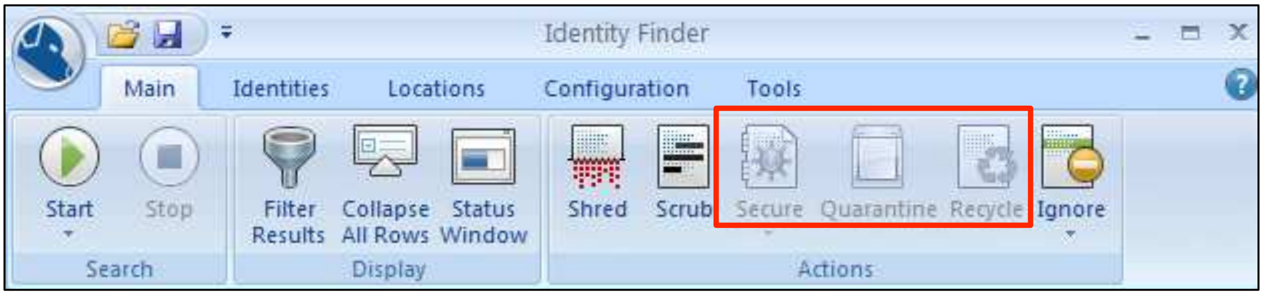

Run a Scan
Identity Finder locates your PII data
Confirmed PII?
No
Ignore
Yes
Do you need to keep this file?
No
Shred
Yes
Do you need to keep PII?
No
Scrub
Yes
Do you need file on your computer?
No
Move to a more secure location
Yes
Full Disk Encryption

- After a user has run a scan, any data that has been determined to be PII will be collected and displayed. From here the user must analyze the data and make a decision on what to do with it.
- In the figure to the left, a flow diagram has been provided to help the user through this process.
- **Ignore** – The ignore option will allow the user to tell Identity Finder to ignore this piece of data, and for this and all subsequent searches run on that computer. This can be used to manage PII that you plan on securing or disposing of by other means, or the function can be used to handle False Positives.
- A false positive is when Identity Finder marks a file that fit the profile of PII, but is actually harmless. This can occur when Identity Finder comes across a set of numbers that may have the same length as a Credit Card number; it is actually just a part of some configuration or maybe a part number for you inventory.
- **Shred** – Users should choose to shred a file when Identity Finder locates a file that is not needed on their computer. By choosing this path for a piece of PII, the user should be sure it is not needed for any reason. Identity Finder's shredding feature is modeled after the US Department of Defense guide lines for data erasure, and the file will not be recoverable once it has been shredded.

If the user finds that they no longer require the PII that may be within a document, but still need the document they may use the ***Scrub*** the file instead. This feature will censor out the PII, but the file will be retained. The ***Scrub*** option can only be performed on certain types of files specifically plain text and non-proprietary file types. Email messages, attachments, PDF files, and files within .zip files cannot be scrubbed. Additionally, the Scrub option will not function on computers running Microsoft Office 2003 or earlier.

Some Options Are Not Available, Why?

During the process of handling any PII that may have been uncovered, you may notice that some functions are not available. Identity Finder offers three features that do handle data differently than the three methods mentioned above. These methods below are disabled by default; however, they may be enabled by request.

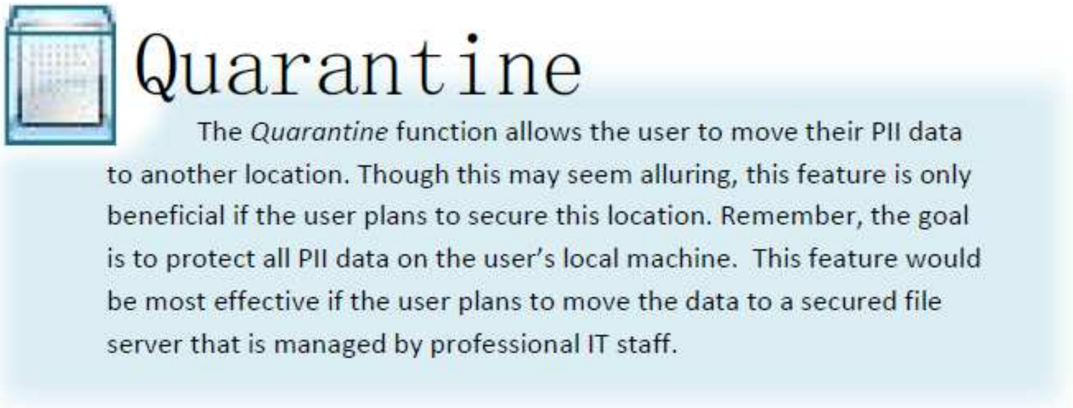


Secure Function:

Secure

The *Secure* function is useful when Identity Finder locates a piece of PII that a user would like to keep on their local machine. The *Secure* feature will encrypt the file and may only be accessed with the password set at the time of encryption. Though this feature may seem advantageous, it may do more harm than good. For example, if a user were to forget the password to the file, the data will not be recoverable.

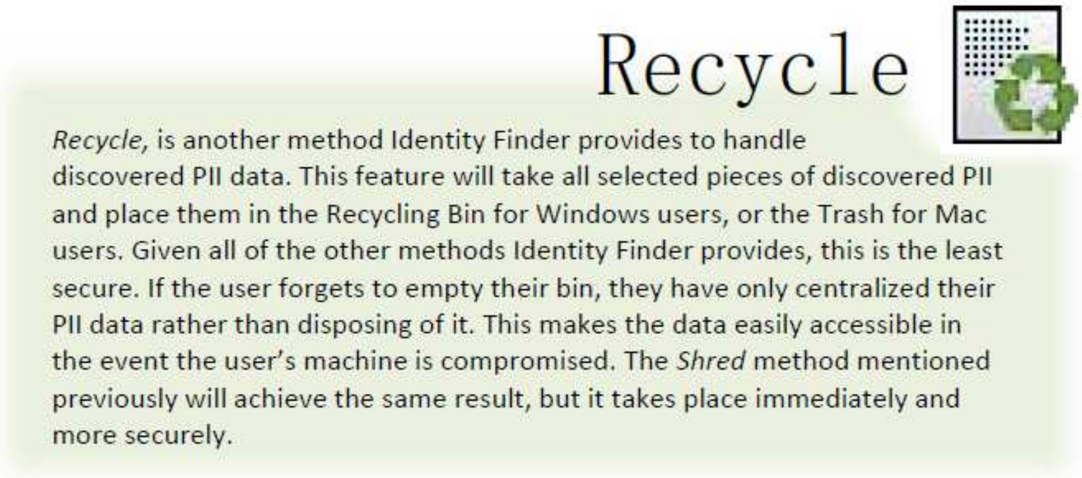
Quarantine Function:



Quarantine

The *Quarantine* function allows the user to move their PII data to another location. Though this may seem alluring, this feature is only beneficial if the user plans to secure this location. Remember, the goal is to protect all PII data on the user's local machine. This feature would be most effective if the user plans to move the data to a secured file server that is managed by professional IT staff.

Recycle Function:



Recycle

Recycle, is another method Identity Finder provides to handle discovered PII data. This feature will take all selected pieces of discovered PII and place them in the Recycling Bin for Windows users, or the Trash for Mac users. Given all of the other methods Identity Finder provides, this is the least secure. If the user forgets to empty their bin, they have only centralized their PII data rather than disposing of it. This makes the data easily accessible in the event the user's machine is compromised. The *Shred* method mentioned previously will achieve the same result, but it takes place immediately and more securely.

Search Types:

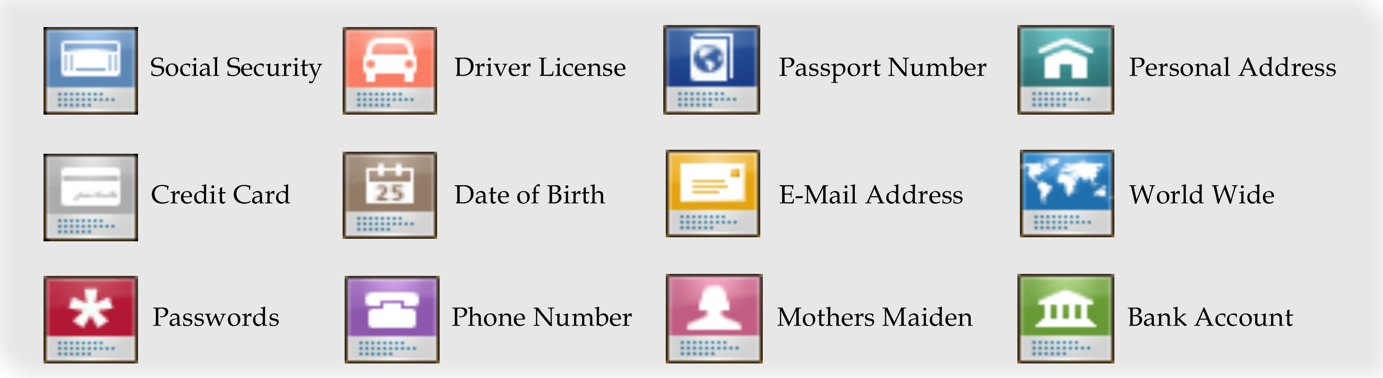
Identity Finder gives the user many robust search types to pick from. The default for the search types are: Social Security, Credit Card and Passwords. However, it is possible to search for all PII types, or pick the types best suited for the user. Identity Finder can also refine its search to specific PII provided by the user. For example, if the user would like to discover any files that may contain their home address, they can provide that information to Identity Finder and it will search for address matching what the user had provided.

The method of searching described in the example above is called an ***OnlyFind***.

- ***OnlyFind*** type searching will only return files that contained PII specific to the information provided by the user.

Identity Finder also offers a nonspecific method of searching called ***AnyFind***.

- ***AnyFind*** will return any file that contains a piece of PII data. This type of the searching is preferable for discovering all PII that may exist on the user's computer.



Advanced Search Types

Identity Finder allows the user to create custom PII types. This is useful for situations where there isn't a predefined PII type for a specific identifier the user is looking for. One use case would be when the user wishes to include the UConn NetID into their search. Identity Finder utilizes ***regular expressions*** to accomplish this. For further information, please have the user contact their technical support staff.