

# Getting Started with Spirion for MAC

## Scanning and Remediation Basics

*Spirion is an application that scans for sensitive data on Windows or MAC computers. Spirion helps USU employees locate and secure sensitive data on their computers. As an important component of data protection at the University, Spirion reduces data exposure and data leakage.*




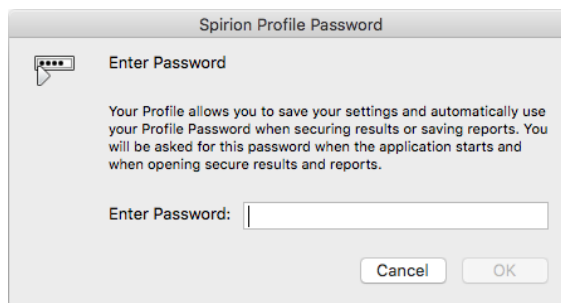
*Frequent use of the Spirion program is important, as it will (1) meet your obligations defined by USU policies and guidelines, (2) help prevent or lessen the severity of a data breach, (3) maintain compliance with state, federal, and international regulations.*

### Contents

- [Spirion Launch and Profile](#)
- [Spirion Scan](#)
- [Remediation \(Data Cleanup\)](#)
- [Common Remediation Options](#)
- [Additional Resources](#)

### Spirion Launch and Profile

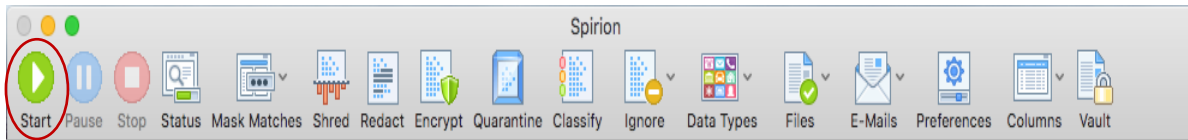
1. Open Spirion by double-clicking the Spirion (Blue Dog) icon in your Applications folder. Go to **Finder**, choose **Applications**, then **Spirion**. Alternatively, you may click on the Spirion application directly from the **Dock**. 
2. You will be prompted to create a Profile. A Profile is optional, but recommended. A Profile will allow access to your secure files, password vault, and search preferences. Most importantly, it will save prior scanned results that are attached to your Profile. The Profile Password must be remembered, as there is no retrieval process. For more information on Spirion Profiles, see [Setting Up Spirion Profiles](#).



- a. If you wish to create a Profile, enter and confirm a new Profile password. Click **OK**.
- b. If you do not wish to create a Profile, click **Cancel**. You will then use the Guest Profile.

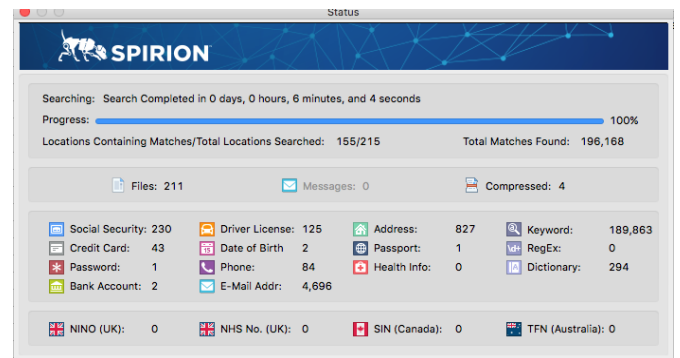
## Spirion Scan

- Once Spirion is open, you may choose the Start button on the toolbar to immediately start your search with the default options (or previously saved options), or you may click the Files button to choose which location you want to search specifically.

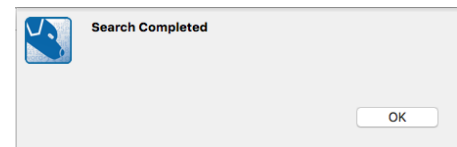


Spirion will begin searching for all data types selected via the **Data Types** button on the toolbar. A **Status Window** will appear to show your current status and results discovered:

*While Spirion is searching in the background, you may continue working on the computer. Spirion should not affect the performance of the computer. You may also interact with results as they appear.*

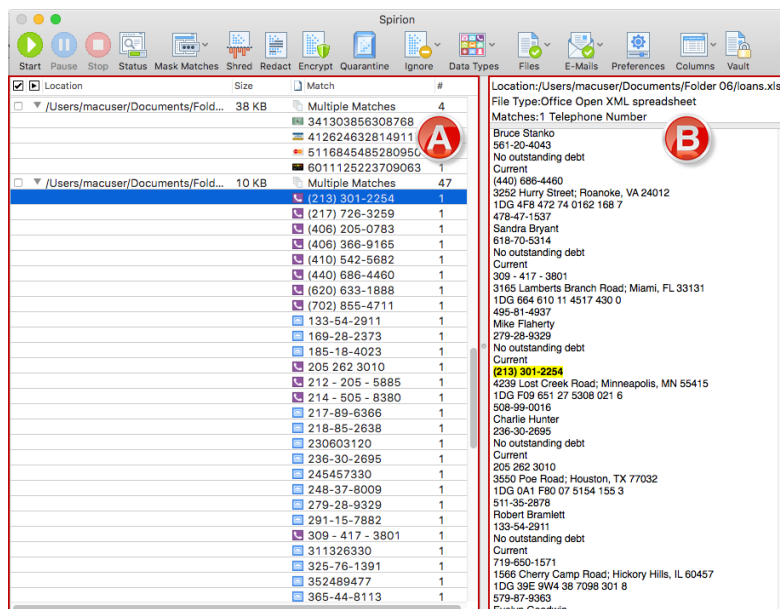


A dialog box will inform you when the search has been completed. Click **OK** to see the search results.



## Remediation (Data Cleanup)

When the scan completes, the Spirion console will display a dialog box with discovered results.



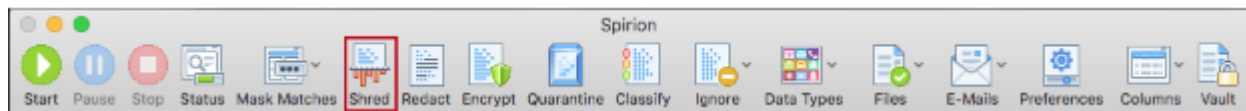
The results of the search are displayed in two areas, the **Results View** and the **Preview Pane**.

A) **Results View** is a reporting table, similar to a spreadsheet (left side of dialog box). This view displays all information about the results of your search and allows you to analyze those results and take action to protect any sensitive information.

B) **Preview Pane** complements the Results View by providing detailed information about the result, including the full path to its location, the type and value of the result, and a preview of the result in context.

## Common Remediation (Data Clean Up) Options

Before you start remediating, please understand the common remediation options described below:



**Shred** – The Shred option permanently deletes the selected files. It bypasses the Recycle Bin, and the file cannot be restored or undone. The file is wiped using a U.S. Department of Defense standard.

**This is the best action if you want to permanently remove an entire file.**

**Redact** – With Redact, Spirion automatically erases the sensitive information, such as Social Security or Credit Card Numbers, and replaces them with a series of Xs. The rest of the document remains untouched. This operation cannot be undone. This option only works on documents containing plain text. It will not work on images or some .pdf documents.

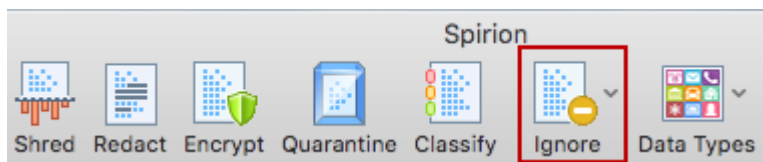
**This is the best action if you want to retain the file but remove the sensitive information.**

**Ignore** – The Ignore option should only be used if Spirion displays a file that contains false positives, meaning the data Spirion thinks is sensitive, yet is not. In a Profile, once data is ignored, the data will not be found on future scans. **Never ignore a document containing sensitive information.** Files with sensitive information should either be shredded, redacted, or moved to a secure location. You should typically ignore by “This Item Location,” which will ignore only that file.

The three common remediation options—**Ignore, Shred, and Redact**—will be discussed further.

### Ignore

Look at each result in detail, to determine if the result is indeed sensitive information. If the file contains sample credit card numbers or certain reported numbers are mistaken for Social Security Numbers, you may tell Spirion to ignore those matches for the current and future searches. Ignored matches are added to an approved exception list—the Ignore List—in your profile so you not see them again unless the file changes significantly. Ignored matches are added to an approved exception list, the **Ignore List**, so you never see them again.



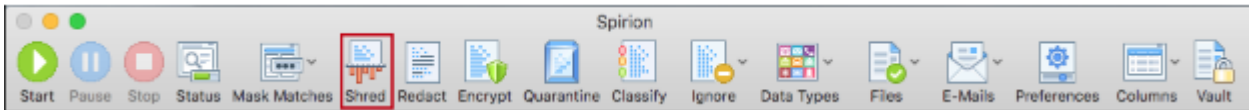
There are four ways to view or manage your **Ignore List** by adding or removing data matches:

1. Click the **Ignore** button on the toolbar, then click on **This Match**.
2. Single click on any result with the right mouse button to highlight it and bring up a context menu, then click **Ignore > This Match**.
3. Manually add the data match to the **Ignore List** by clicking the **Preferences** button on the toolbar and selecting the **Ignore** button.
4. Manually add the data match to the **Ignore List** by clicking the **Ignore** button on the toolbar, then click on **Manage 'Ignore List'...**

Because ignored data matches may contain sensitive information, the list is stored in your Profile.

## Shred

When a location has a sensitive data match and you wish to permanently remove it from your computer, use the **Shred** feature. **Shred** is the correct choice when you no longer need the sensitive information.

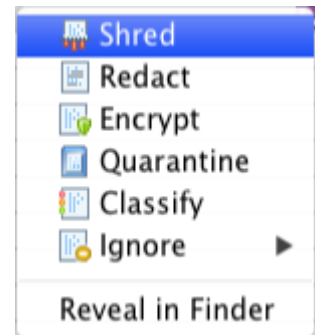


The **Shred** button is located on the toolbar and is enabled for all types of results. **Shred** utilizes a secure United States Department of Defense wiping standard known as DOD 5220.22-M.

*Note: Shredded results cannot be recovered. Once you shred something, it is gone.*

There are two ways to **Shred** a location:

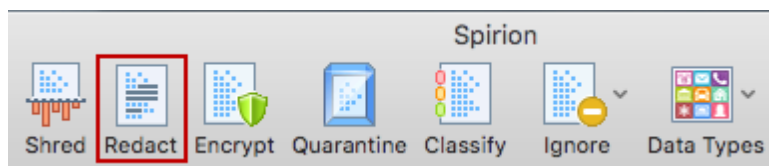
1. Single click the result with the left mouse button to highlight it and click the **Shred** button on the toolbar.
2. Single click the result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on **Shred**.



## Redact

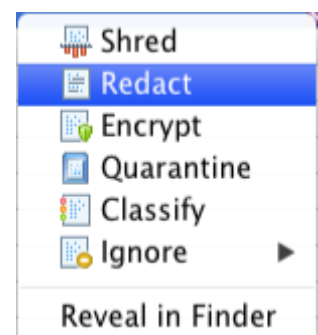
When a file contains sensitive information and you wish to keep the item but remove the sensitive information only, you should utilize the **Redact** feature. **Redact** is great when you no longer need the sensitive information but want to keep the original item.

*Note: Redact is only available for specific file types searched via the Files search and is not available for E-Mail or other search locations. You may only scrub Office 2007 and higher files (e.g., docx, xlsx, pptx) and text files (i.e., \*.txt, \*.log, \*.ini).*



The Redact button is located on the toolbar and is enabled for certain file types. There are two ways to **Redact** a location:

1. Single click the result with the left mouse button to highlight it and click the **Redact** button on the toolbar.
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 **Redact**.



After you have addressed each item in the Results Pane, please rescan your device or drive to ensure you have cleaned all sensitive information from your computer device or drives.

## Additional Resources

Since only the basics have been covered in the document, please review the additional Spirion resources are available in the following locations:

- USU [Spirion@USU KnowledgeBase](#) Article
- USU [Learning Management](#) System. Type “Spirion” in Search box after login
- Spirion Detailed [User Manual](#)
- USU IT Help Desk, 435.797.HELP
- In-house Training; contact the [Data Privacy Office](#)

USU will prompt University-wide Spirion searches throughout the year. Therefore, if the Spirion (Blue Dog) icon appears in your task bar, without your starting a search, please do not worry. Let the program scan and run. Spirion can slow large processing jobs, but generally, you should see little difference in your computer performance. Learn more about [Computer Performance with Spirion](#).

Although central scans are initiated, **it is ultimately your responsibility to ensure Spirion scans are run**. Frequent scans will help detect sensitive data, which must be removed from computer devices and drives, and placed in secure USU-approved systems.

For control purposes, the USU Data Privacy Office recommends that you run a manual Spirion scan monthly or weekly, depending on the amount of data handled and the sensitivity of the data.



Thank you for using Spirion. Spirion protects you in your job functions by discovering and securing sensitive information.