Product release: January 2023

Scalable Rules for Automatic and Manual Security Classification

Torsion Administrators can now set Security Classifications on Information Resources within Microsoft 365 using the new Scalable Rules for Automatic and Manual Security Classifications.

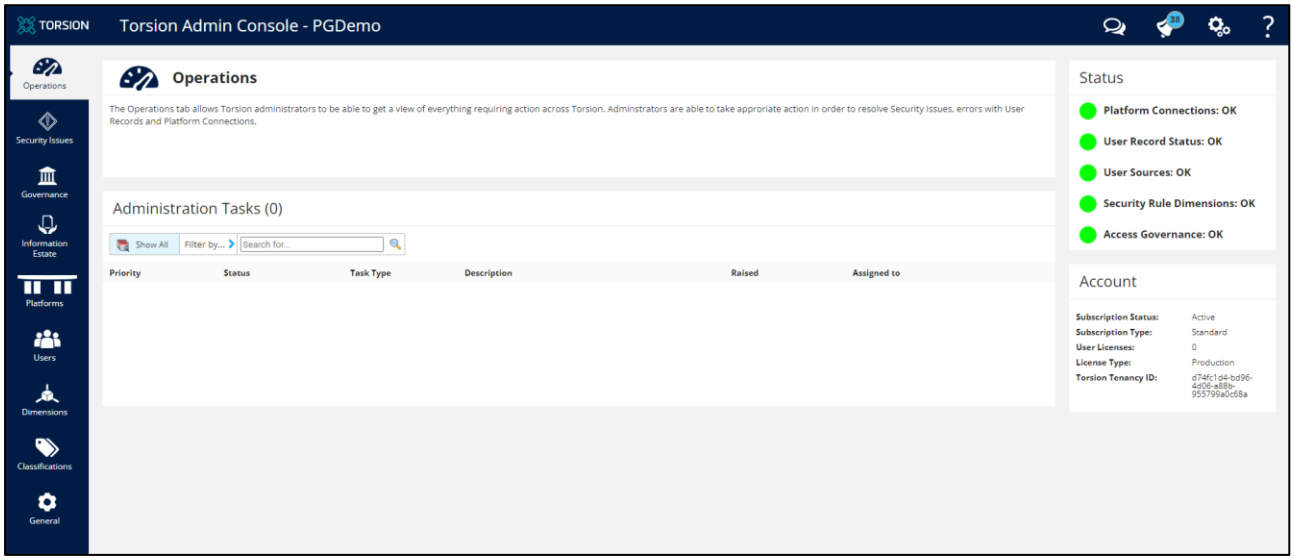
Security classifications guide your business's users to understand the purpose, audience, and sensitivity of business's data.

The classification scheme is formed by the set of Security Classifications, that should be designed in accordance with your information governance policies and your existing information architecture.

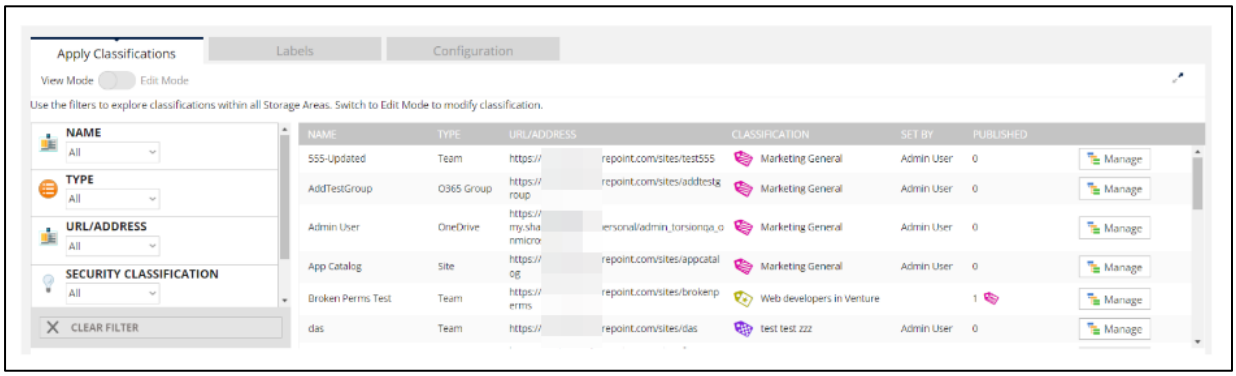
Sharing configurations can be associated to Classification Labels and will be applied to information when it is classified.

So, how do the new Scalable Rules for Automatic and Manual Security Classification work in practise?

From the Torsion Administration Console



Select the Classifications button from the side panel of the left-hand side.

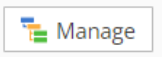


There are two modes of Security Classifications, View Mode and Edit Mode

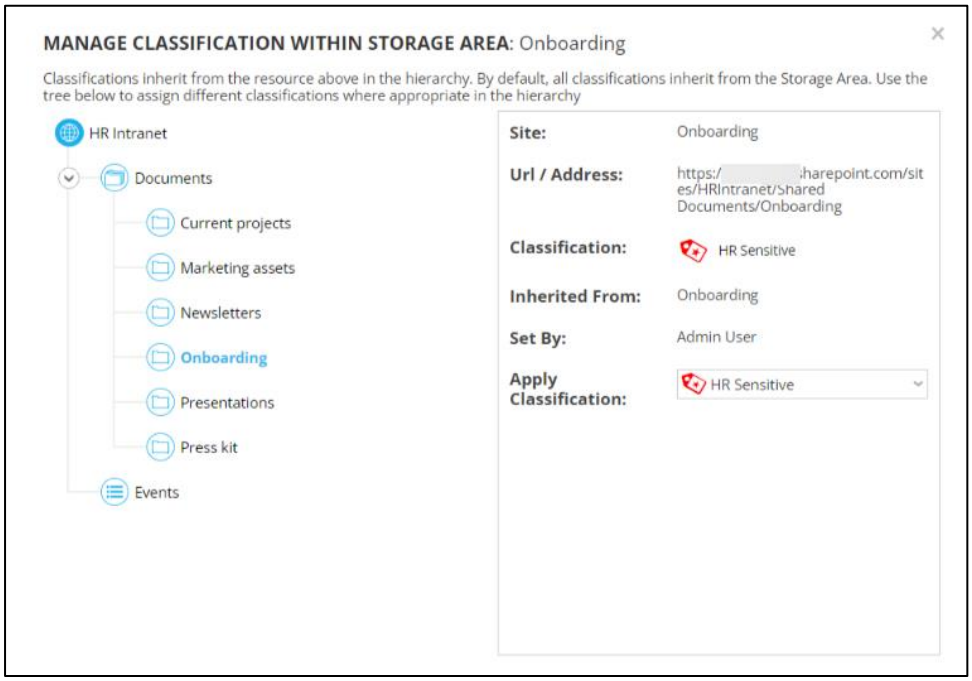
View Mode

View Mode allows for the existing Security Classification Rules to be Viewed or Managed.

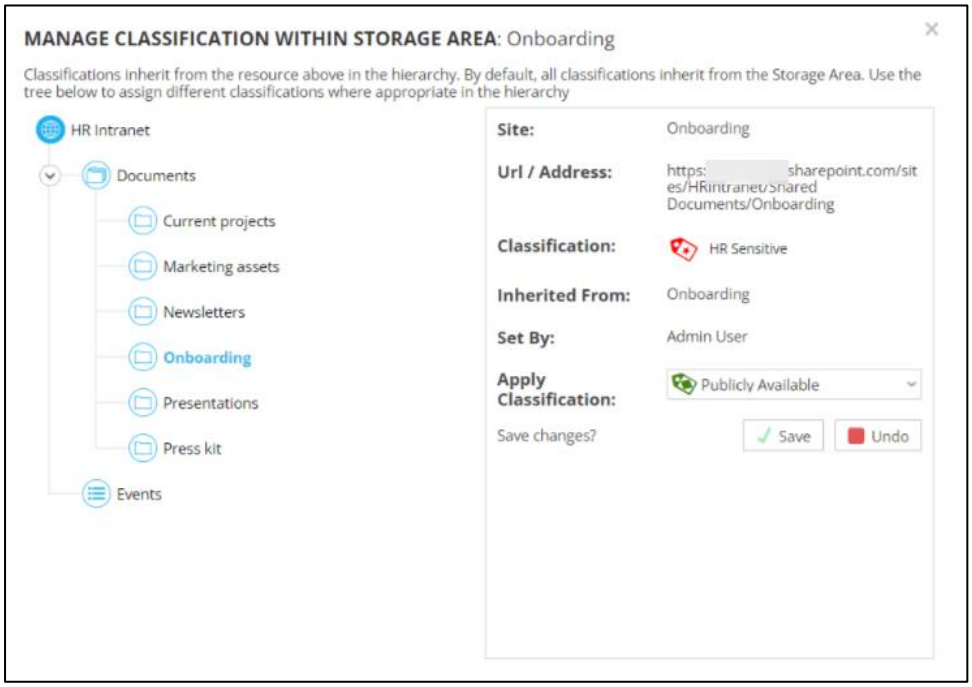
In the example above the HR Intranet Site has been classified as HR Sensitive by the Admin User.

Select the Manage button. 

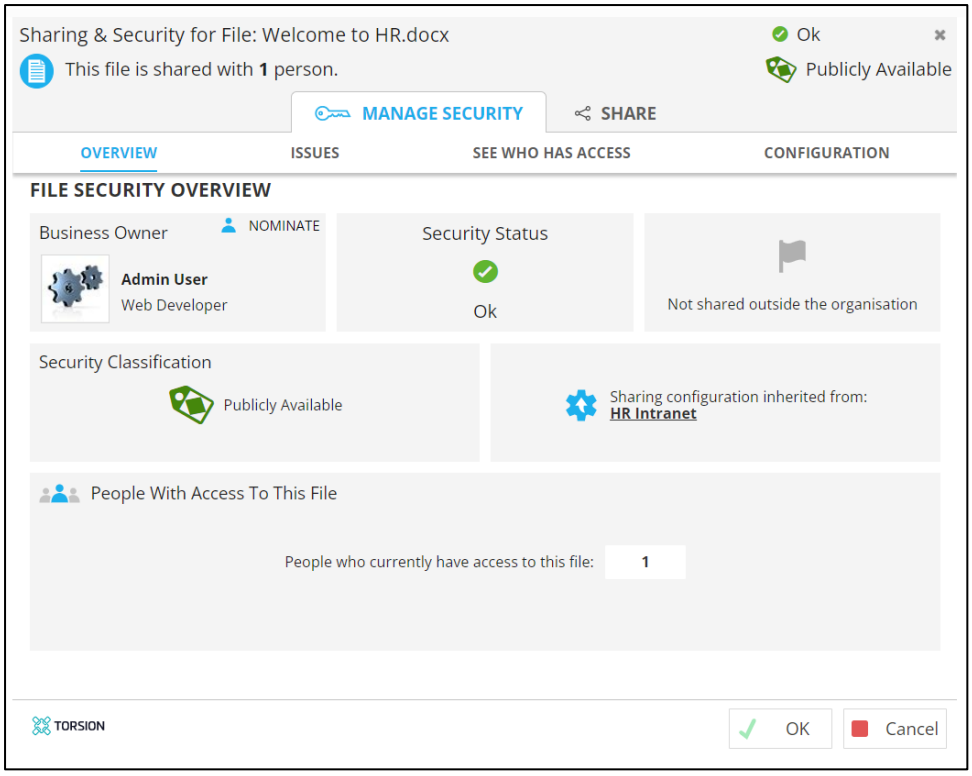
Below we can see that the Security Classification “HR Sensitive” has been inherited to all of the folders contained within the Documents library.



Below is an example of a document library with six folders. The folder Onboarding folder has been Classified as Publicly Available.



Here's an example of the view a Business User would see from the Torsion Sharing and Security panel. This is for the document named “Welcome to HR.docx”, which is saved in the Onboarding folder.

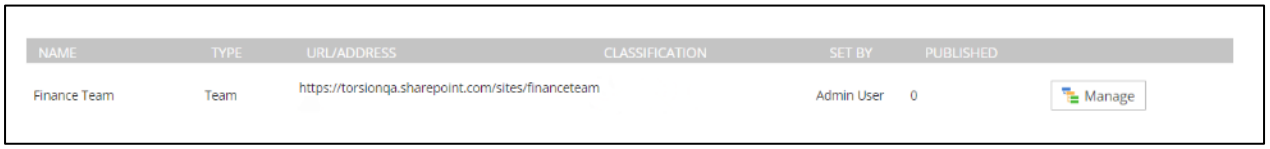


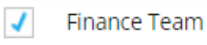
Edit Mode

Manual and Automatic Security Classifications can be applied in Edit Mode.

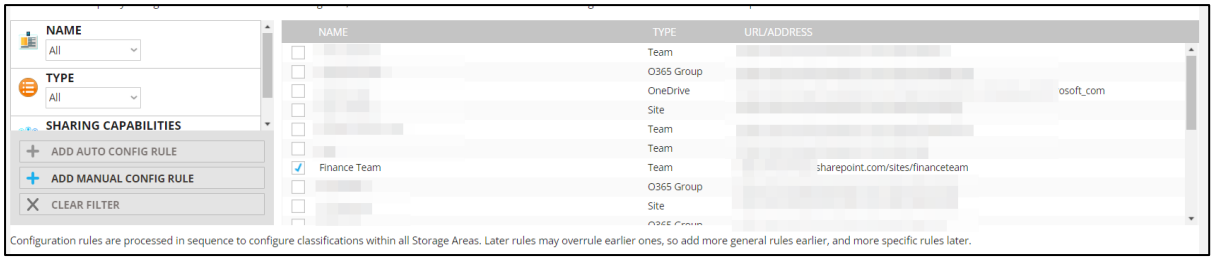
Add a Manual Config Rule

In the example below we are going to Manually apply the Security Classification Finance Sensitive to the Finance Team

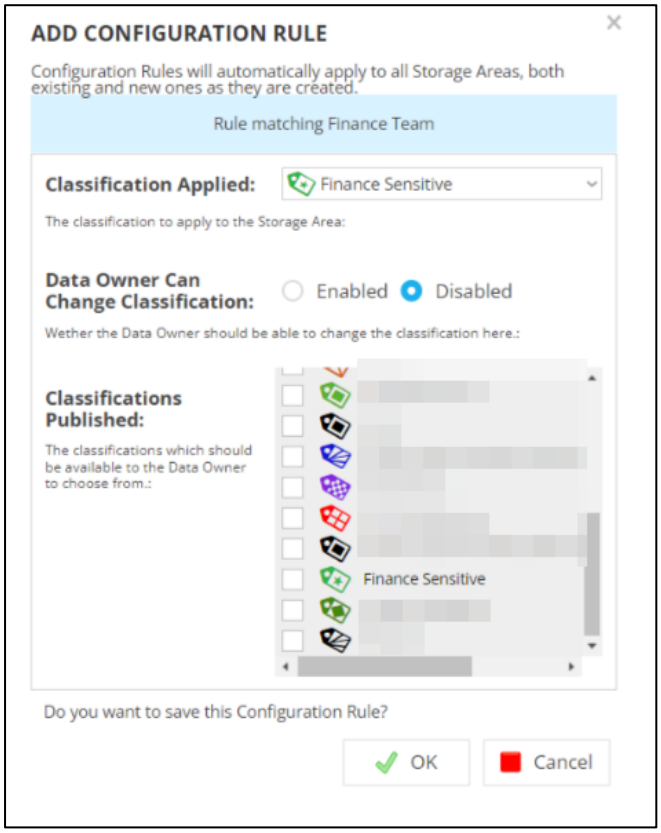


Select the Finance Team 

and select the Add Manual Config Rule 

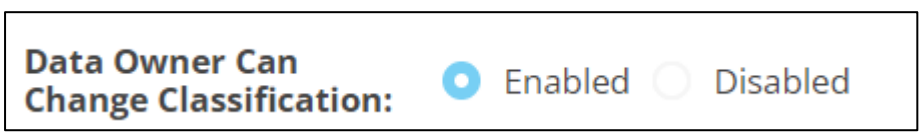


In this example, Data Owners are not allowed to change the Classification.

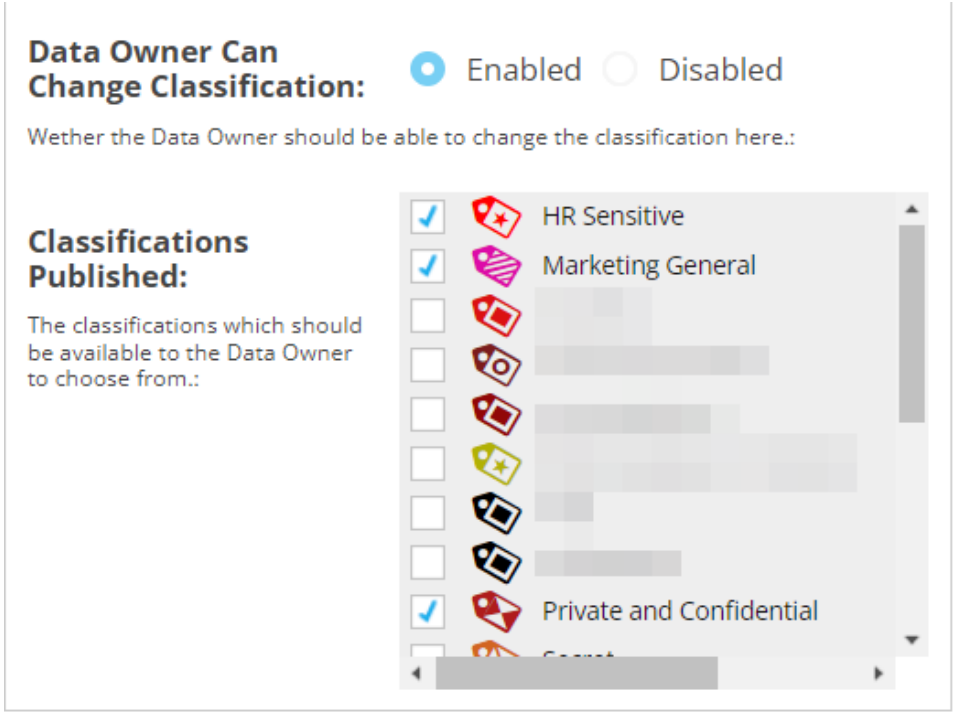


The Finance Team is classified as Finance Sensitive

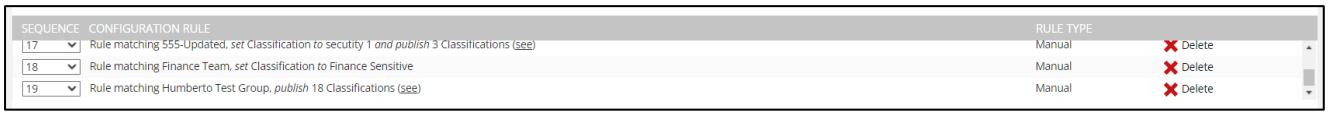
Allowing Data Owners to allocate Published Security Classifications



Using the function to allow Data Owners to Change Classification. Security Classifications can be published to Information Resources.



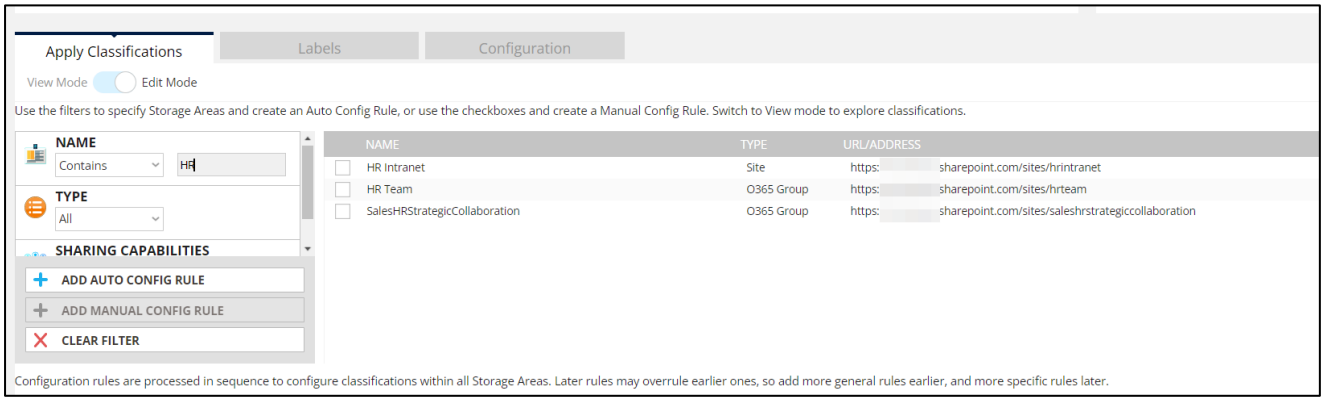
The Information Resource's Business Owner can now choose to apply Security Classifications from those which have been made available to those Information Resources.



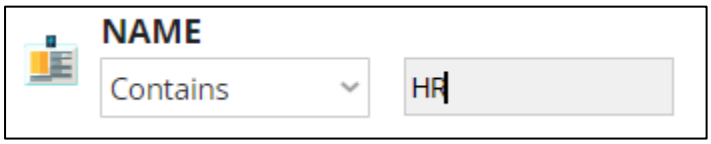
Please be aware that configuration rules are processed in sequence to configure classifications within all Storage Areas. Later rules may overrule earlier ones, so add more general rules earlier, and more specific rules later.

Add an Auto Config Rule

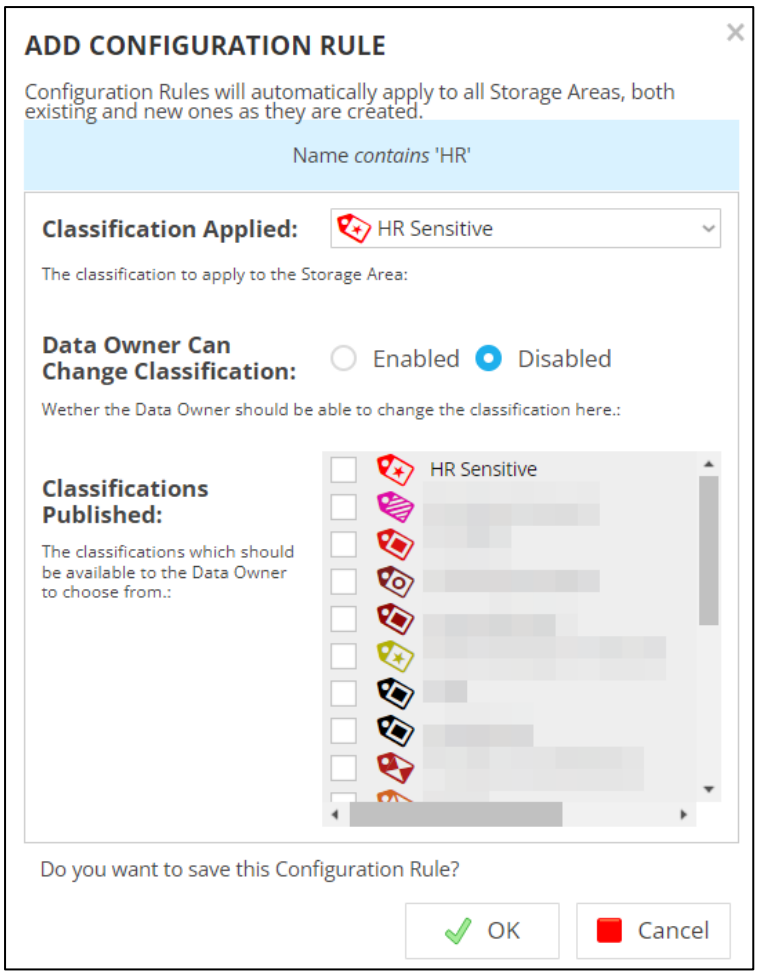
Auto config rule work from the filters for Name, Type and Sharing Capability



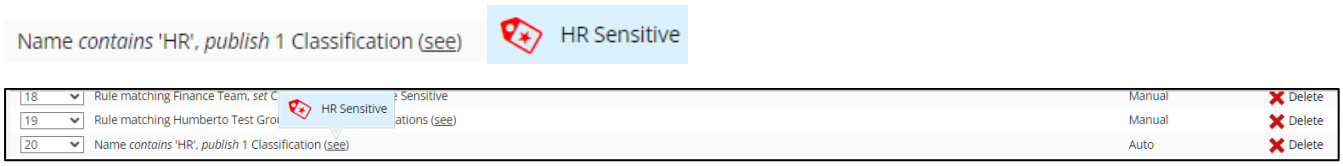
In this example we will create an Auto Config for all the Information Resources that contain the letters “HR”.



Select  ADD AUTO CONFIG RULE



Any Information Resource which name contains the letters “HR” will now be Classified as “HR Sensitive”



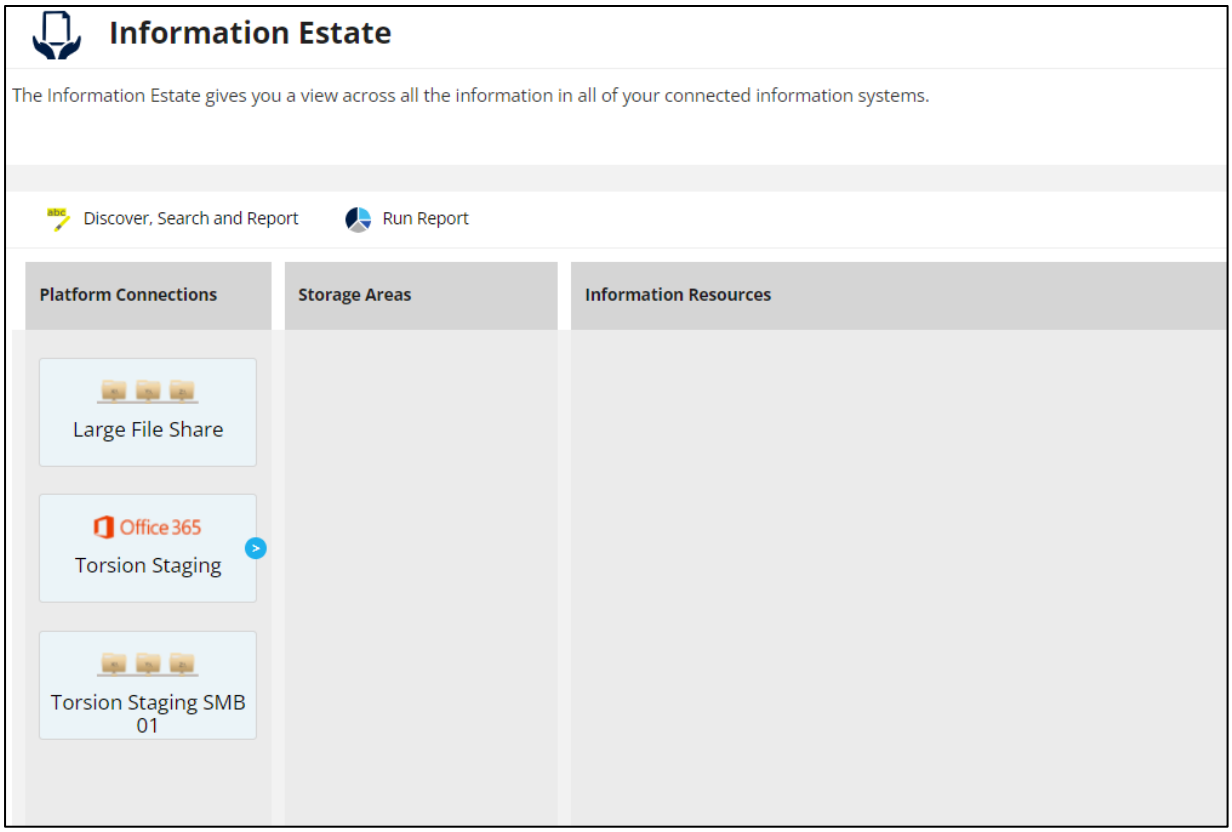
Please be aware that configuration rules are processed in sequence to configure classifications within all Storage Areas. Later rules may overrule earlier ones, so add more general rules earlier, and more specific rules later.

Discovering where Security Classifications are being used

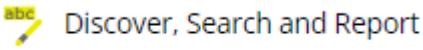
Form the Torsion Administration Console

Select the Information Estate button from the side panel on the left-hand side.

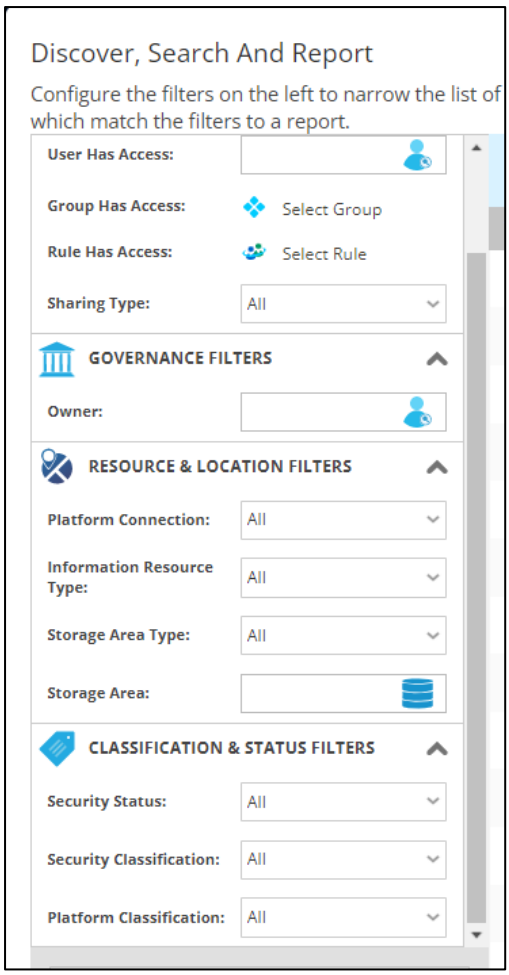
You should now see a screen that looks like this.



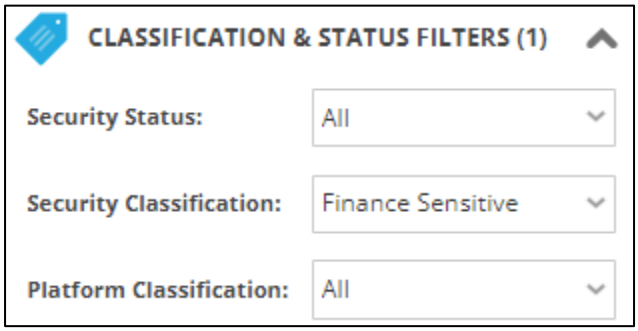
Select the button Discover, Search and Report



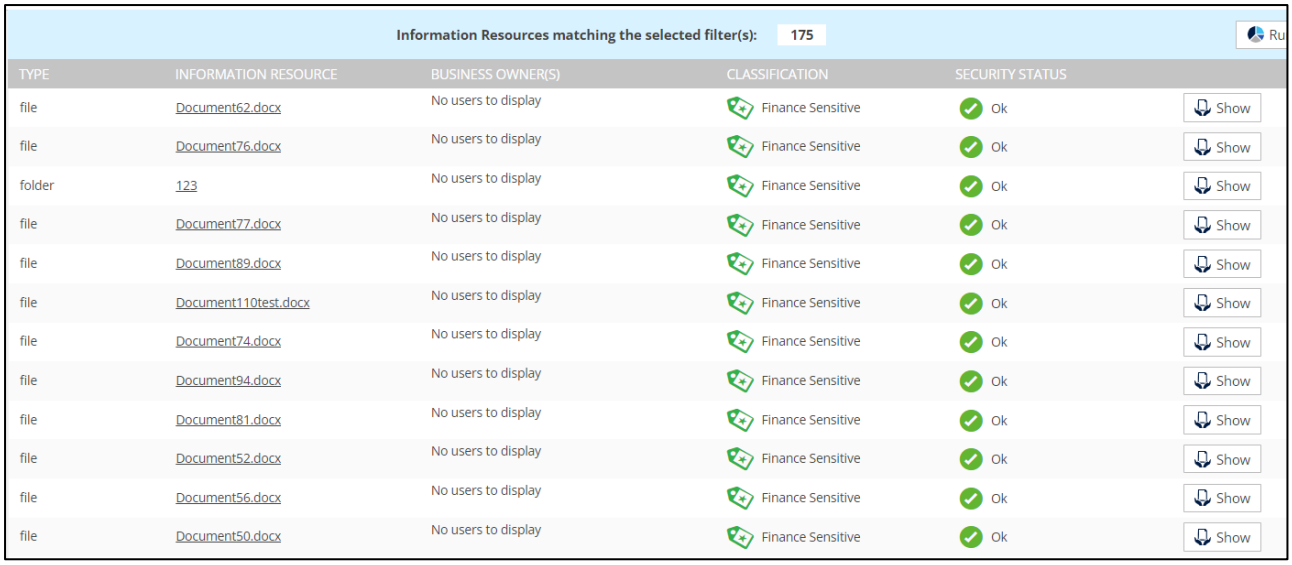
Select the Classification & Status Filters



In the following example, I've chosen Finance Sensitive as the Security Classification to filter on.



This now displays a list of all the data that has been designated as Finance Sensitive.



Information Resources matching the selected filter(s): 175

TYPE	INFORMATION RESOURCE	BUSINESS OWNER(S)	CLASSIFICATION	SECURITY STATUS	
file	Document62.docx	No users to display	Finance Sensitive	Ok	Show
file	Document76.docx	No users to display	Finance Sensitive	Ok	Show
folder	123	No users to display	Finance Sensitive	Ok	Show
file	Document77.docx	No users to display	Finance Sensitive	Ok	Show
file	Document89.docx	No users to display	Finance Sensitive	Ok	Show
file	Document110test.docx	No users to display	Finance Sensitive	Ok	Show
file	Document74.docx	No users to display	Finance Sensitive	Ok	Show
file	Document94.docx	No users to display	Finance Sensitive	Ok	Show
file	Document81.docx	No users to display	Finance Sensitive	Ok	Show
file	Document52.docx	No users to display	Finance Sensitive	Ok	Show
file	Document56.docx	No users to display	Finance Sensitive	Ok	Show
file	Document50.docx	No users to display	Finance Sensitive	Ok	Show

To view more details, select