



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

Torsion Admin Console - PGDemo

Operations

The Operations tab allows Torsion administrators to be able to get a view of everything requiring action across Torsion. Administrators are able to take appropriate action in order to resolve Security Issues, errors with User Records and Platform Connections.

Administration Tasks (0)

Show All Filter by... Search for...

Priority	Status	Task Type	Description	Raised	Assigned to
----------	--------	-----------	-------------	--------	-------------

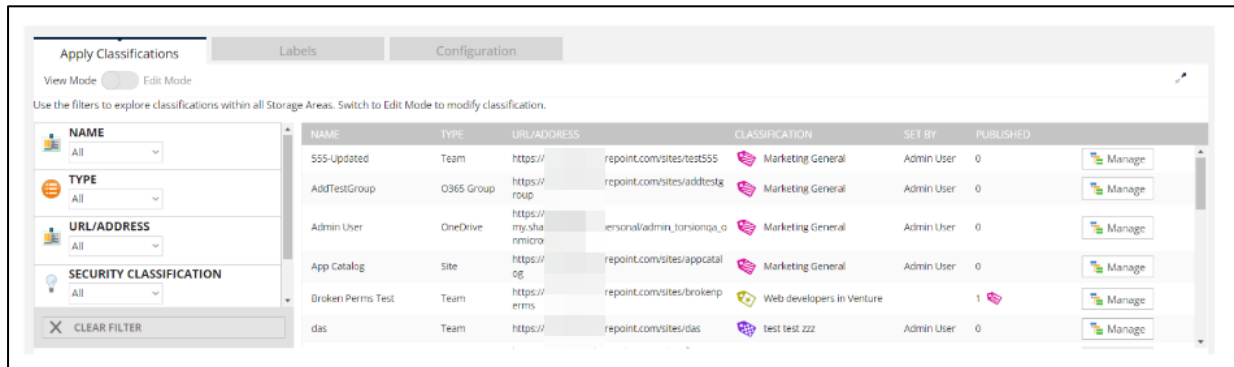
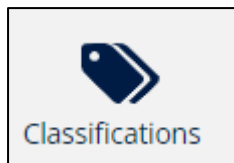
Status

- Platform Connections: OK
- User Record Status: OK
- User Sources: OK
- Security Rule Dimensions: OK
- Access Governance: OK

Account

Subscription Status: Active
Subscription Type: Standard
User Licenses: 0
License Type: Production
Torsion Tenancy ID: 0745c104-b496-4e05-a88b-955799a0c58a

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

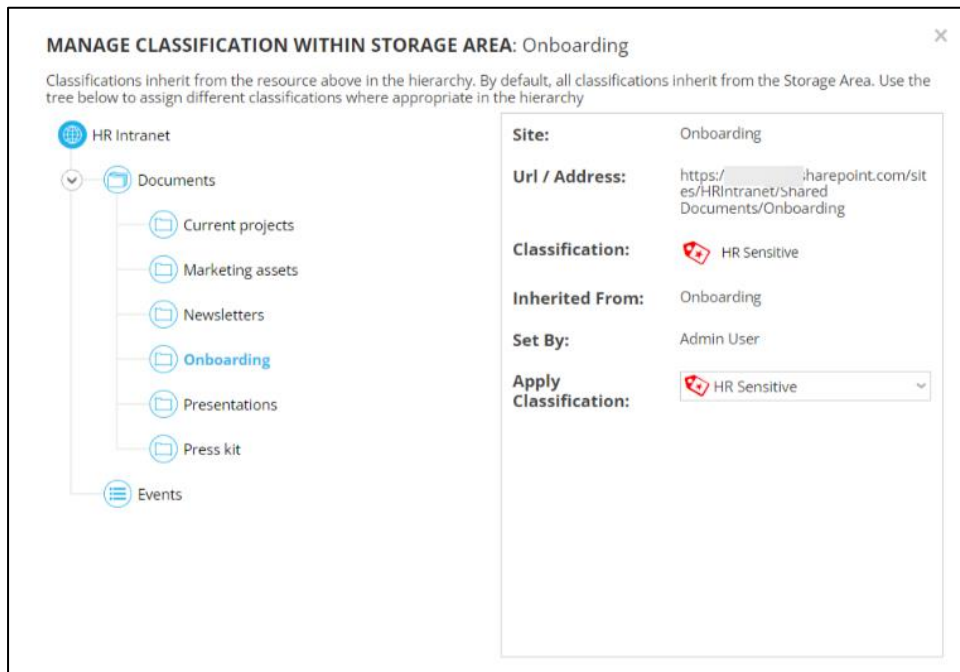
View Mode allows for the existing Security Classification Rules to be Viewed or Managed.

NAME	TYPE	URL/ADDRESS	CLASSIFICATION	SET BY	PUBLISHED	
HR Intranet	Site	https://sharepoint.com/sites/hrintranet	HR Sensitive	Admin User	0	Manage

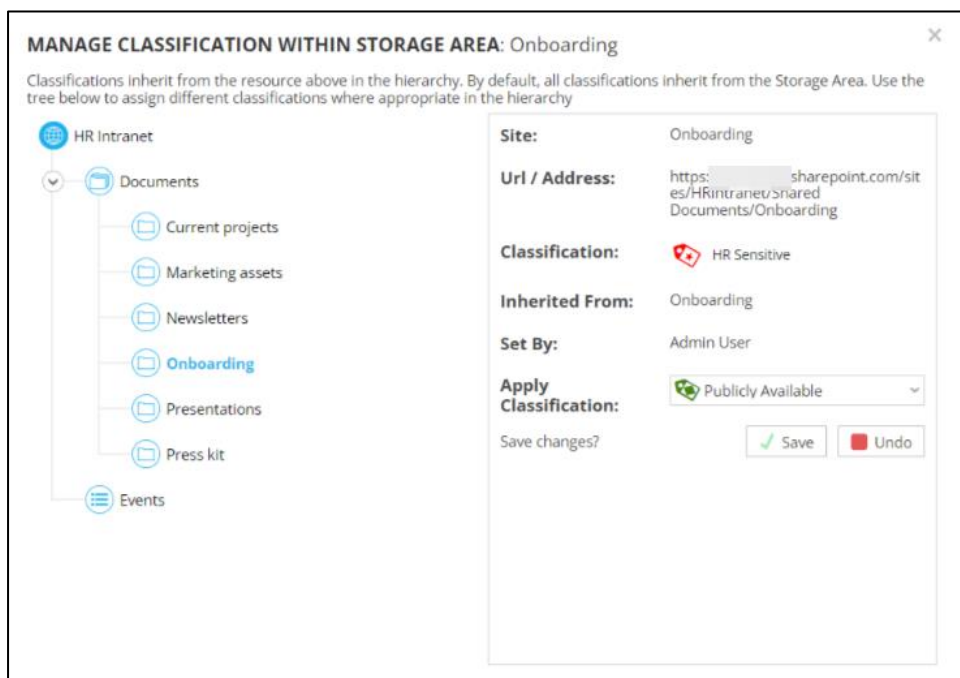
In the example above the HR Intranet Site has been classified as HR Sensitive by the Admin User.

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.

Sharing & Security for File: Welcome to HR.docx

Ok

Publicly Available

This file is shared with 1 person.

MANAGE SECURITY

SHARE

OVERVIEW

ISSUES

SEE WHO HAS ACCESS

CONFIGURATION

FILE SECURITY OVERVIEW

Business Owner

NOMINATE

Admin User

Web Developer

Security Status

Ok

Not shared outside the organisation

Security Classification

Publicly Available

Sharing configuration inherited from:

HR Intranet

People With Access To This File

People who currently have access to this file:

1

TORSION

OK

Cancel

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

NAME	TYPE	URL/ADDRESS	CLASSIFICATION	SET BY	PUBLISHED	
Finance Team	Team	https://torsionqa.sharepoint.com/sites/financeteam		Admin User	0	Manage

Select the Finance Team ☒ Finance Team

and select the Add Manual Config Rule [+ ADD MANUAL CONFIG RULE](#)

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

Data Owner Can Change Classification:

EnabledDisabled

Wether the Data Owner should be able to change the classification here.:

Classifications Published:

The classifications which should be available to the Data Owner to choose from.:

HR Sensitive

Marketing General

Private and Confidential

Secret

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

SEQUENCE	CONFIGURATION RULE	RULE TYPE	
17	Rule matching 555-Updated, set Classification to security 1 and publish 3 Classifications (see)	Manual	Delete
18	Rule matching Finance Team, set Classification to Finance Sensitive	Manual	 Delete
19	Rule matching Humberto Test Group, publish 18 Classifications (see)	Manual	Delete

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

Apply Classifications

Labels

Configuration

View Mode

Edit Mode

Use the filters to specify Storage Areas and create an Auto Config Rule, or use the checkboxes and create a Manual Config Rule. Switch to View mode to explore classifications.

NAME

Contains

HR

TYPE

All

SHARING CAPABILITIES

+

ADD AUTO CONFIG RULE

+

ADD MANUAL CONFIG RULE

×

CLEAR FILTER

NAME	TYPE	URL/ADDRESS
☐ HR Intranet	Site	https://sharepoint.com/sites/hrintranet
☐ HR Team	O365 Group	https://sharepoint.com/sites/hrteam
☐ SalesHRStrategicCollaboration	O365 Group	https://sharepoint.com/sites/saleshrstrategiccollaboration

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.

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

NAME

Contains

HR

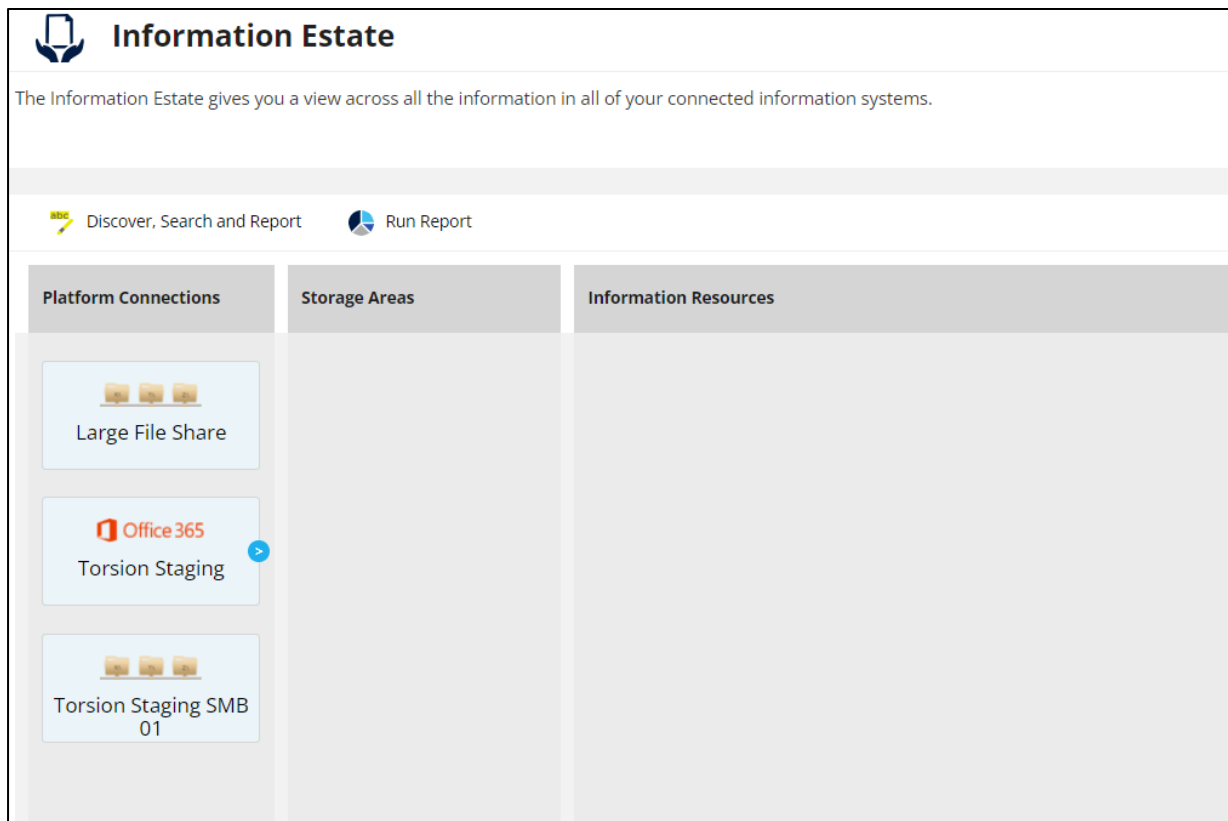
Select

+

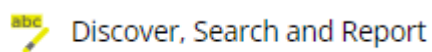
 ADD AUTO CONFIG RULE



You should now see a screen that looks like this.



Select the button Discover, Search and Report



Select the Classification & Status Filters

Discover, Search And Report

Configure the filters on the left to narrow the list of which match the filters to a report.

User Has Access:

Group Has Access:

Select Group

Rule Has Access:

Select Rule

Sharing Type:

All

 **GOVERNANCE FILTERS**

Owner:

 **RESOURCE & LOCATION FILTERS**

Platform Connection:

All

Information Resource Type:

All

Storage Area Type:

All

Storage Area:

 **CLASSIFICATION & STATUS FILTERS**

Security Status:

All

Security Classification:

All

Platform Classification:

All

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

 **CLASSIFICATION & STATUS FILTERS (1)**

Security Status:

All

Security Classification:

Finance Sensitive

Platform Classification:

All

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 [Show](#)

