Sensitivity labels - what do they look like

Heidi Hasting

Senior Consultant

Exposé

SQL SATURDAY

2022 Oregon & SW Washington

Heidi Hasting

exposé
Data Exposed

@HeidiHasting
www.heidihasting.com

- Business Intelligence Professional formerly software developer.

- ALM/DLM enthusiast and Azure DevOps Fan
- Regular attendee at tech events

Sensitivity labels - what do they look like

- Like me you may have heard about sensitivity labels but what does that mean to your reports, data or documents. Some of the questions this session will answer;
  - what do they look like in Power BI
  - what do they look like in Azure SQL
  - what do they look like in Azure Purview
  - what do they look like in 0365
  - how to maintain and manage them

  In this session we will go through setting up sensitivity labels and see them across multiple platforms (Power BI, Azure Purview)

What are sensitivity labels?

> *“Information Protection helps organizations discover, classify, label, and protect sensitive documents and emails. Admins can define rules and conditions to apply labels automatically, users can apply labels manually, or a combination of the two can be used—where users are given recommendations on applying labels.”*
>
> Microsoft 365 guidance for security & compliance - Service Descriptions | Microsoft Docs

- As the name implies they are Labels!
- Labels that can be applied to various things
  - Office files (word, excel, power point)
  - Power BI reports (.pbix)
- Can be used to provide additional protection (security)

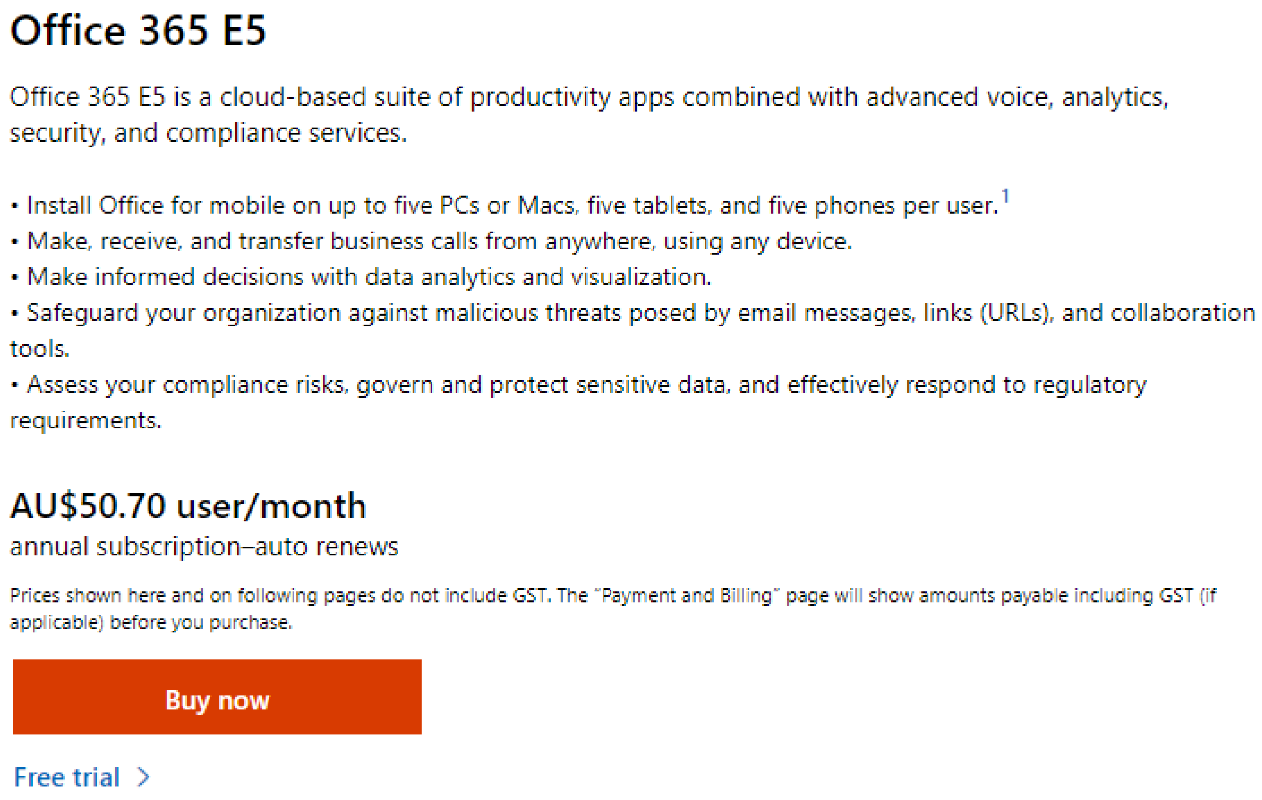
Licensing (urgh ☹)

Multiple licensing scenarios depending on setup

- Power BI has specific requirements

See link at end of presentation for more options

Users need
Power BI Pro
or
Premium Per User



Office 365 E5

Office 365 E5 is a cloud-based suite of productivity apps combined with advanced voice, analytics, security, and compliance services.

- Install Office for mobile on up to five PCs or Macs, five tablets, and five phones per user.[1]
- Make, receive, and transfer business calls from anywhere, using any device.
- Make informed decisions with data analytics and visualization.
- Safeguard your organization against malicious threats posed by email messages, links (URLs), and collaboration tools.
- Assess your compliance risks, govern and protect sensitive data, and effectively respond to regulatory requirements.

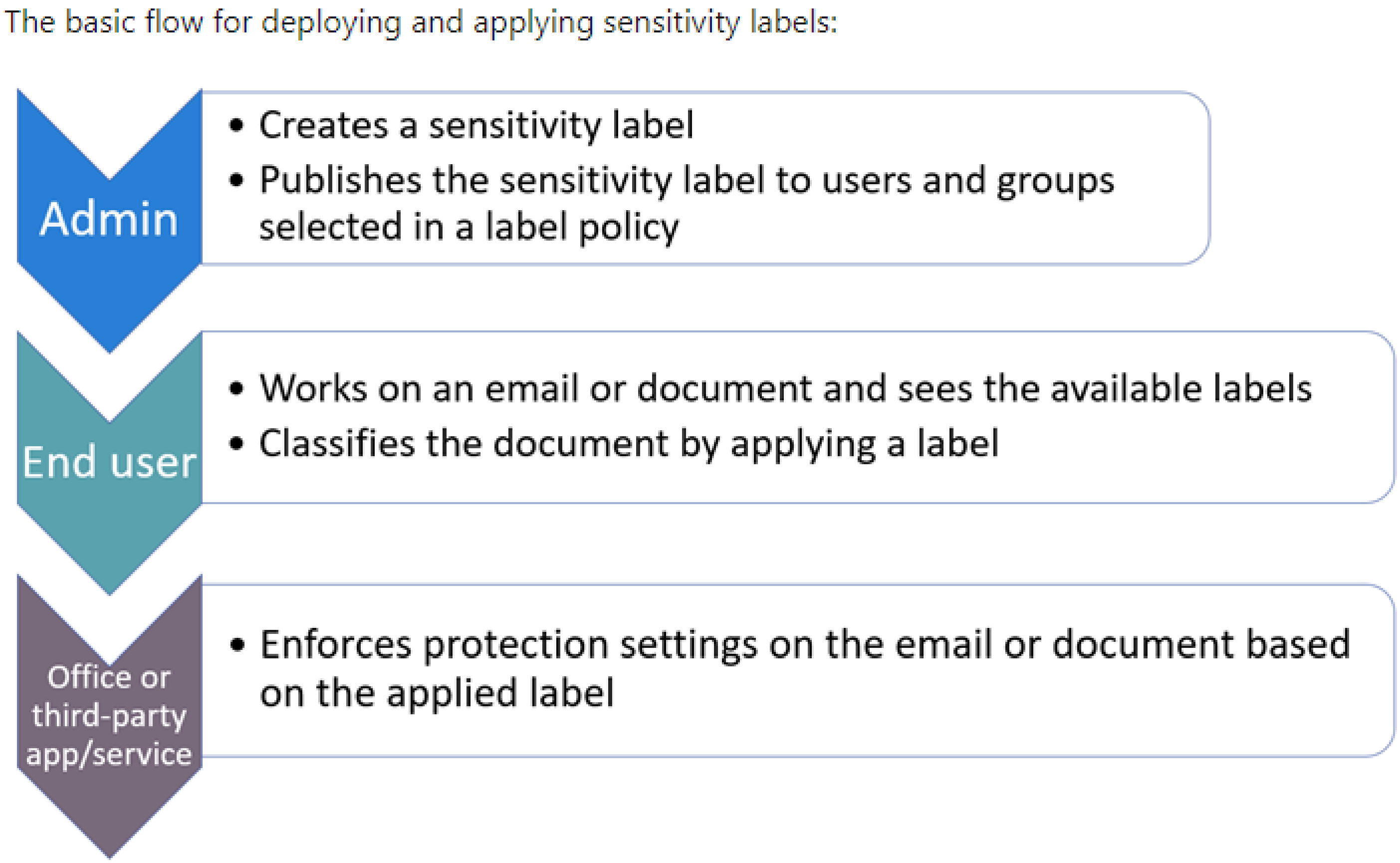
AU$50.70 user/month

annual subscription–auto renews

Prices shown here and on following pages do not include GST. The "Payment and Billing" page will show amounts payable including GST (if applicable) before you purchase.

https://www.microsoft.com/en-au/microsoft-365/enterprise/office-365-e5?activetab=pivot%3aoverviewtab

Process



The basic flow for deploying and applying sensitivity labels:

Admin

- Creates a sensitivity label
- Publishes the sensitivity label to users and groups selected in a label policy

End user

- Works on an email or document and sees the available labels
- Classifies the document by applying a label

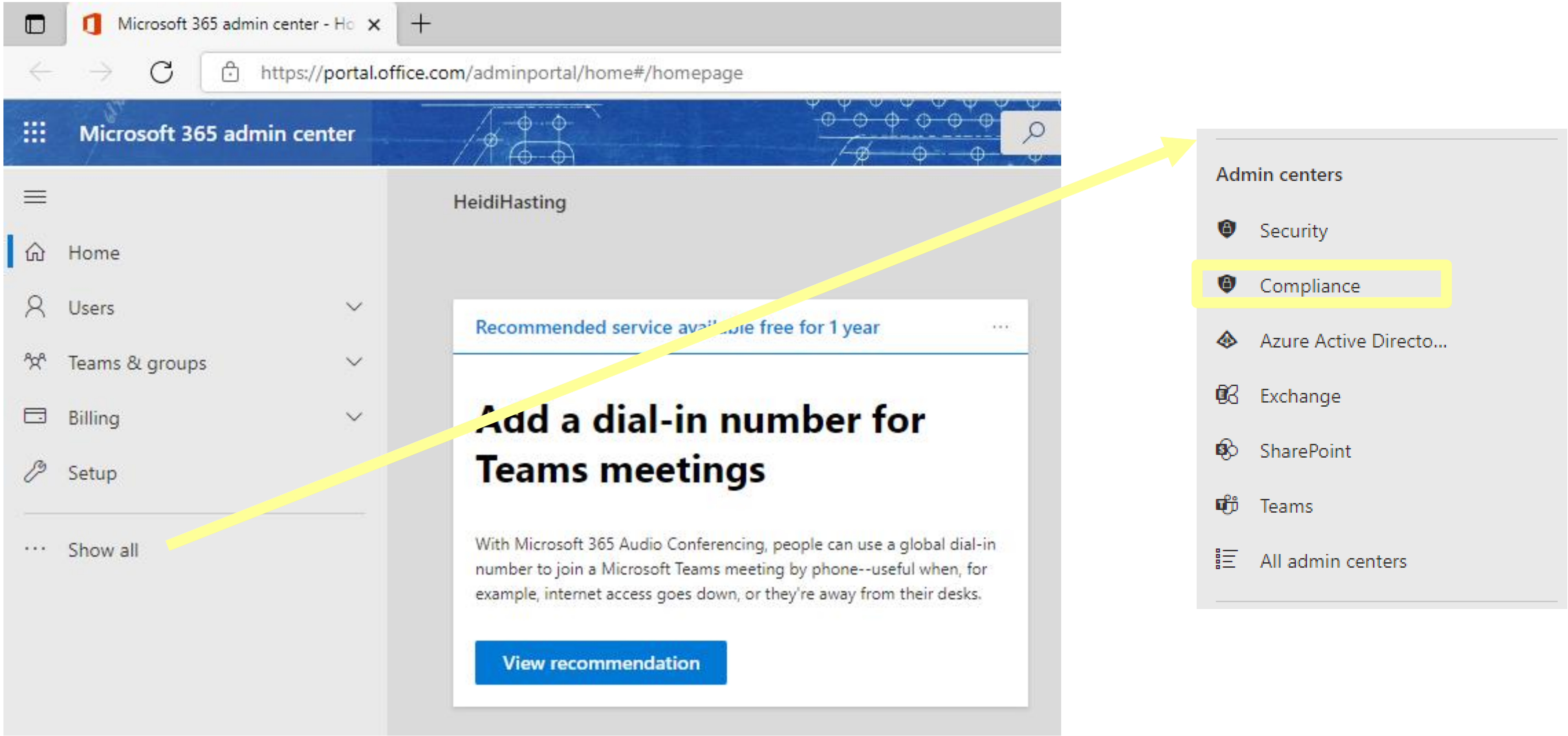
Office or third-party app/service

- Enforces protection settings on the email or document based on the applied label

https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide#subscription-and-licensing-requirements-for-sensitivity-labels

SETUP & MANAGEMENT

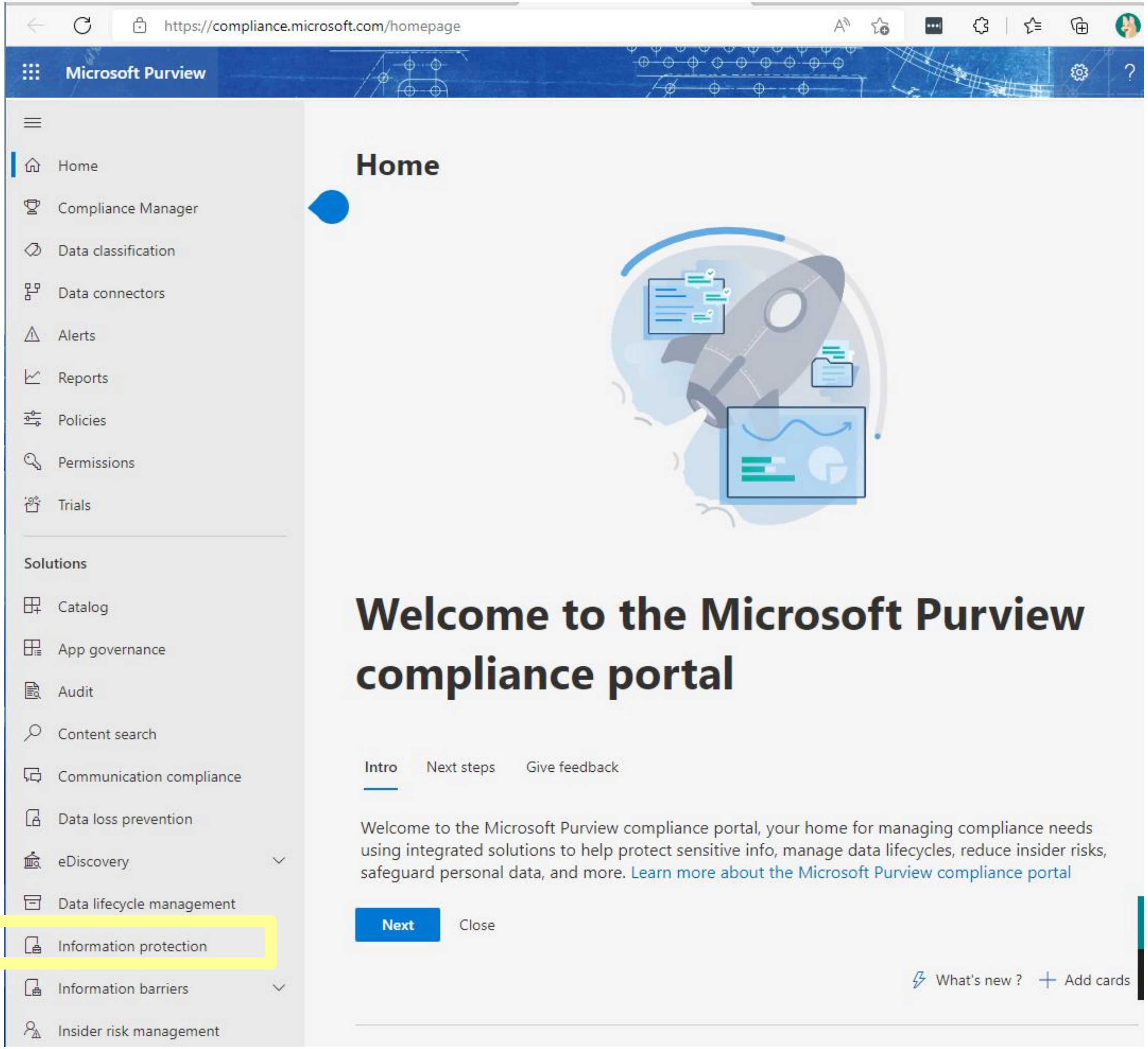
O365 Admin Centre



Add a dial-in number for Teams meetings

With Microsoft 365 Audio Conferencing, people can use a global dial-in number to join a Microsoft Teams meeting by phone--useful when, for example, internet access goes down, or they're away from their desks.

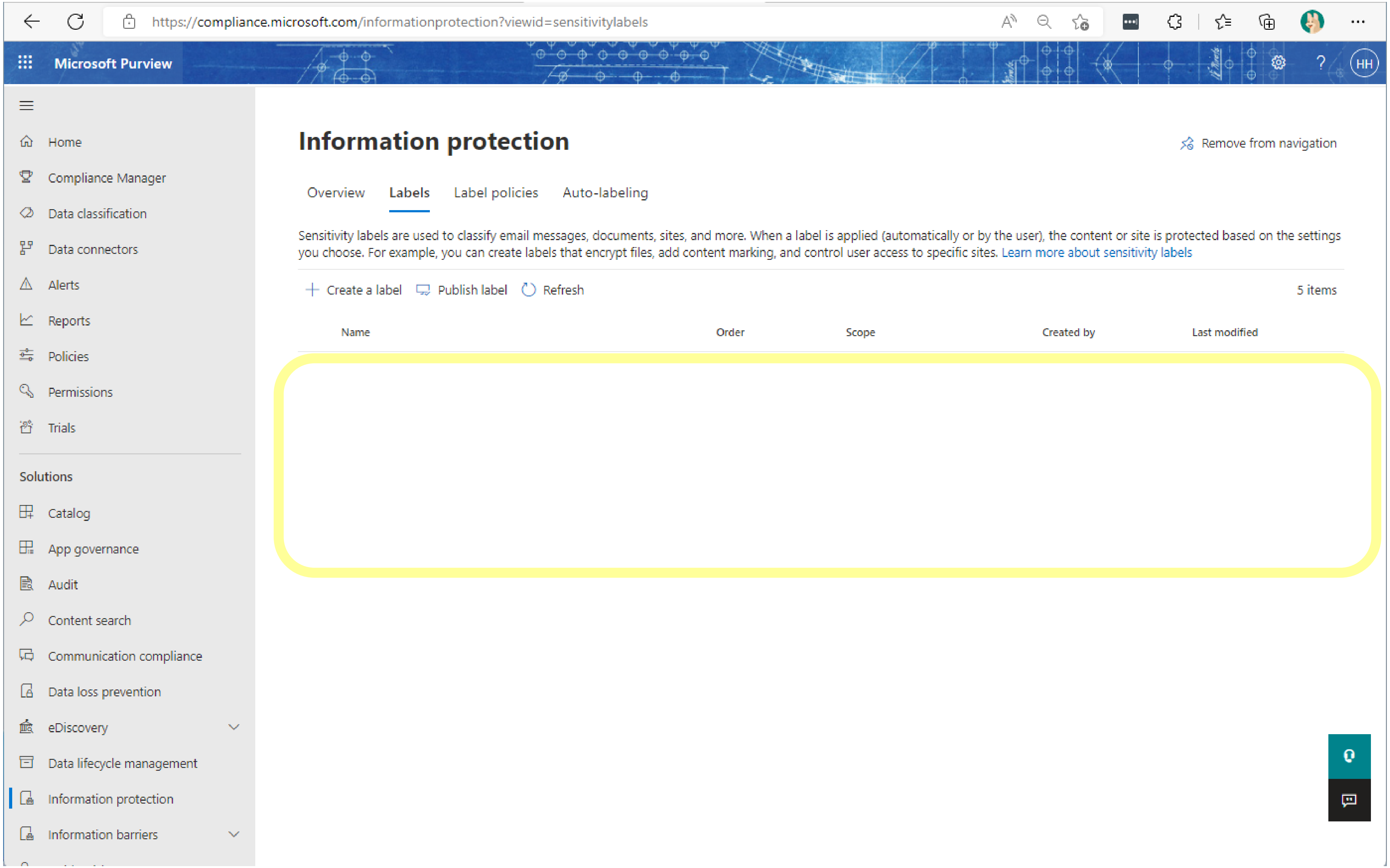
https://portal.office.com/adminportal/home#/homepage



Home

Welcome to the Microsoft Purview compliance portal

Welcome to the Microsoft Purview compliance portal, your home for managing compliance needs using integrated solutions to help protect sensitive info, manage data lifecycles, reduce insider risks, safeguard personal data, and more. Learn more about the Microsoft Purview compliance portal



Information protection

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

Name	Order	Scope	Created by	Last modified

Create a label

Label properties (name, description)

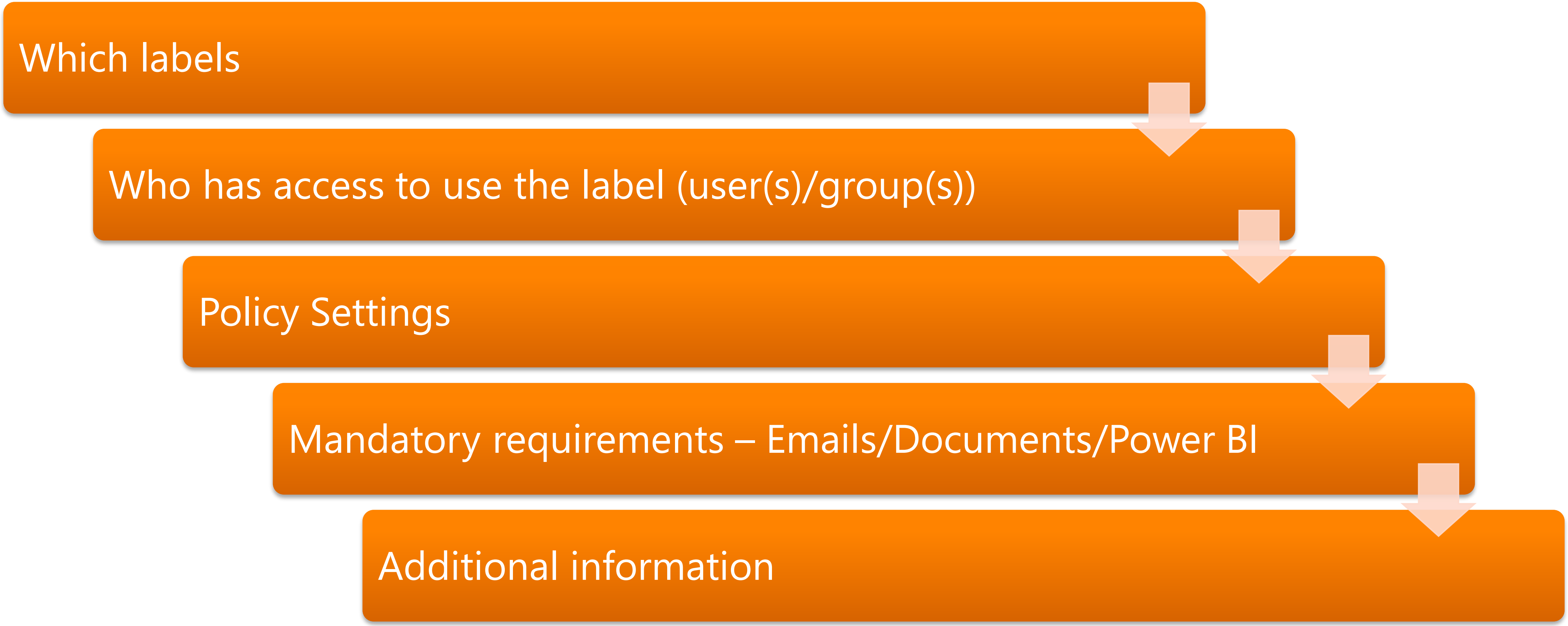
Scope (files, groups & sites, Azure Purview / Azure SQL…)

Protection for files (encrypt, watermark)

Encryption (expiry, offline access, permission)

Publish

Publish a label (create a policy)



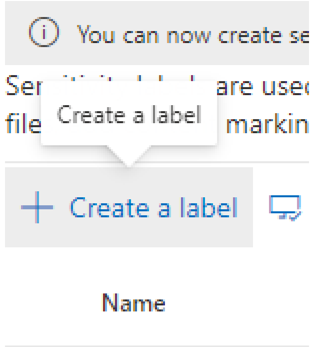
Which labels

Who has access to use the label (user(s)/group(s))

Policy Settings

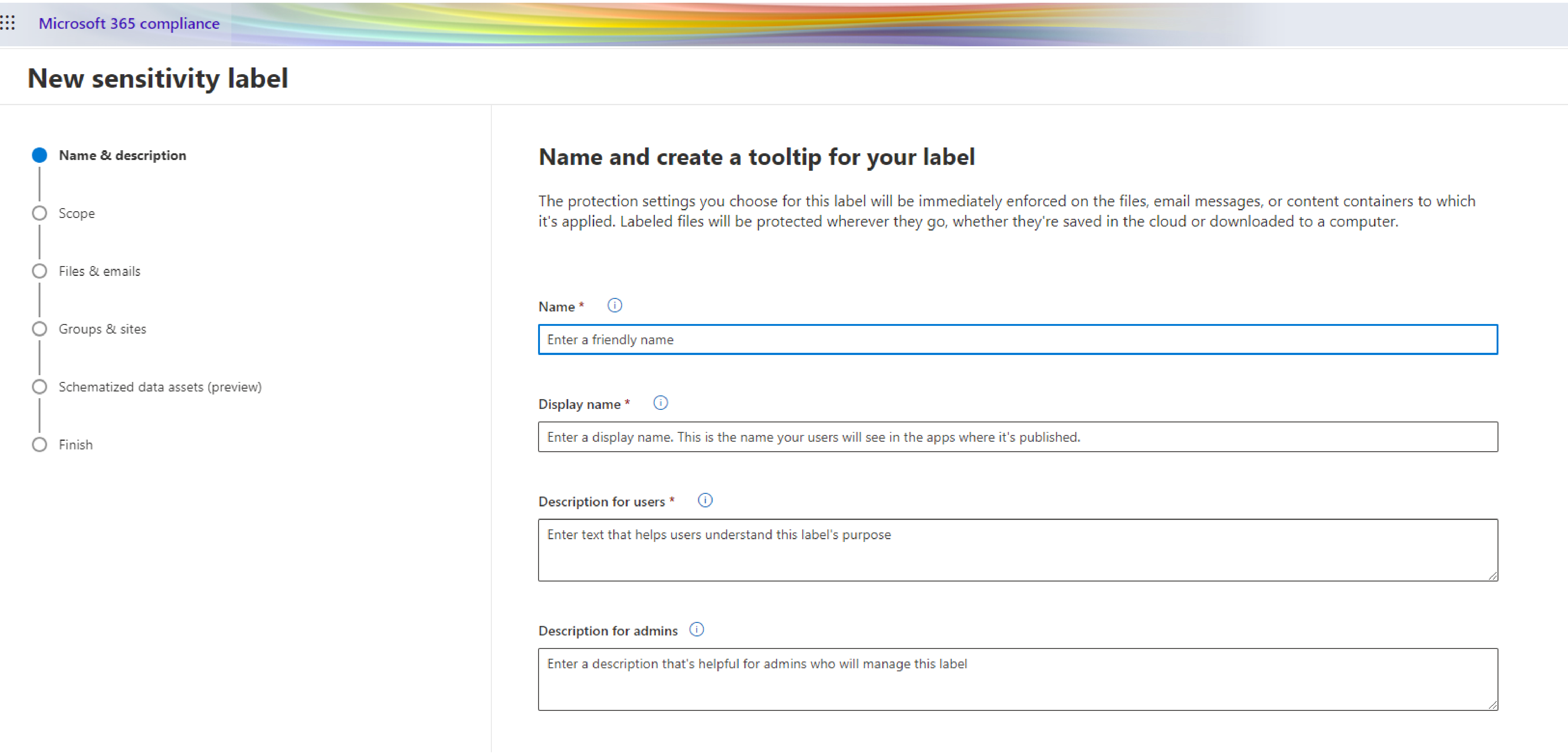
Mandatory requirements – Emails/Documents/Power BI

Additional information



You can now create se

Ser are usec
file markin



New sensitivity label

- ● **Name & description**
- ○ Scope
- ○ Files & emails
- ○ Groups & sites
- ○ Schematized data assets (preview)
- ○ Finish

Name and create a tooltip for your label

The protection settings you choose for this label will be immediately enforced on the files, email messages, or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name * ⓘ

Enter a friendly name

Display name * ⓘ

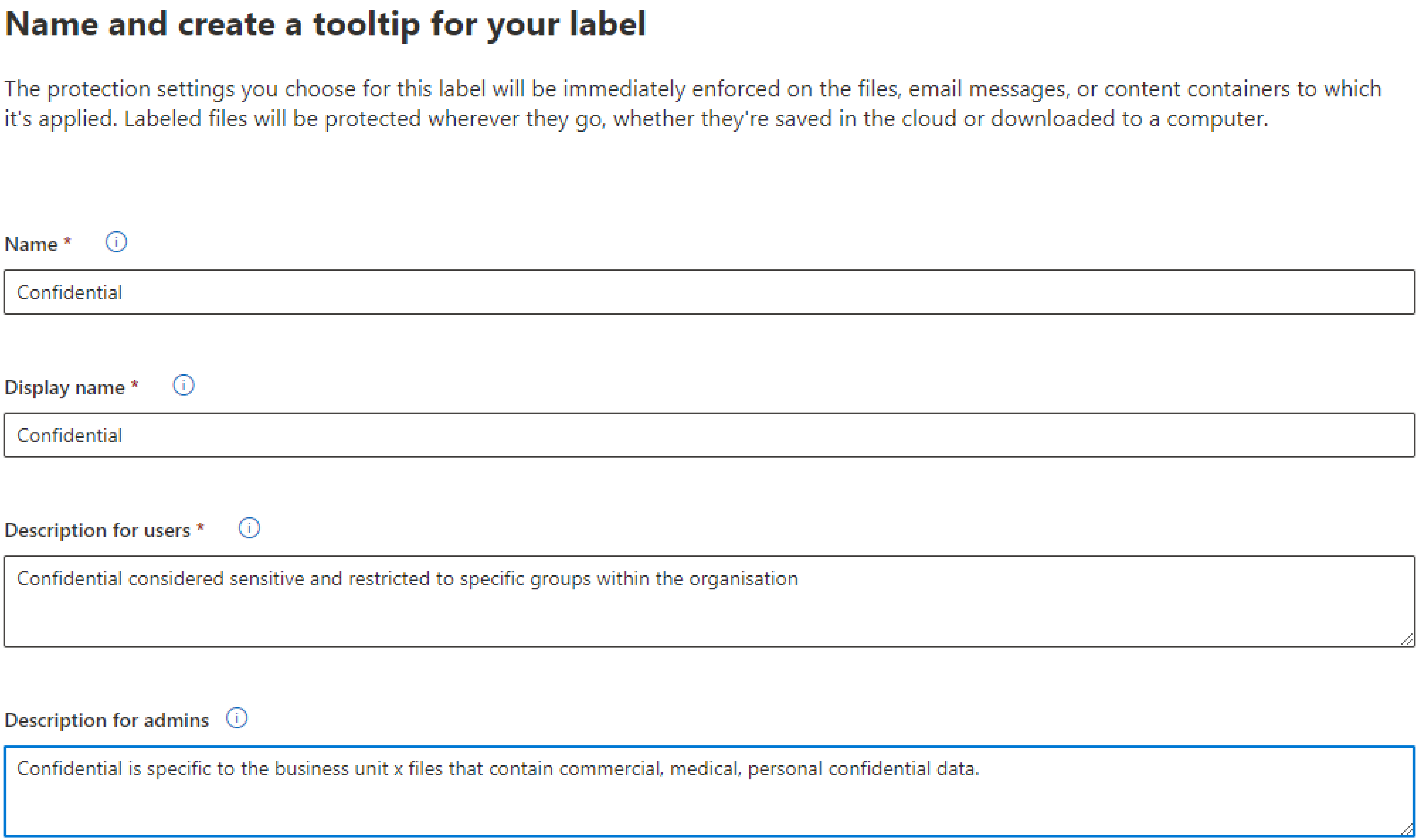
Enter a display name. This is the name your users will see in the apps where it's published.

Description for users * ⓘ

Enter text that helps users understand this label's purpose

Description for admins ⓘ

Enter a description that's helpful for admins who will manage this label



Name and create a tooltip for your label

The protection settings you choose for this label will be immediately enforced on the files, email messages, or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name *

Confidential

Display name *

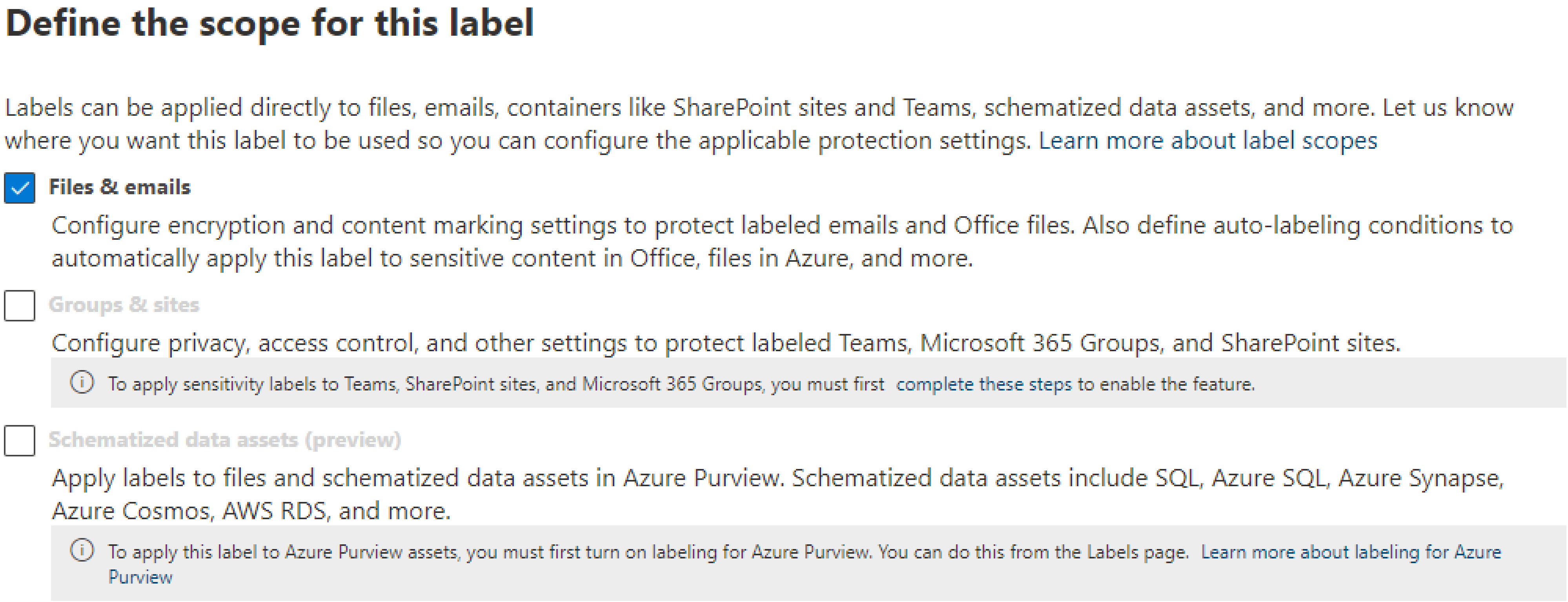
Confidential

Description for users *

Confidential considered sensitive and restricted to specific groups within the organisation

Description for admins

Confidential is specific to the business unit x files that contain commercial, medical, personal confidential data.



Define the scope for this label

Labels can be applied directly to files, emails, containers like SharePoint sites and Teams, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. Learn more about label scopes

☑ **Files & emails**

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

□ **Groups & sites**

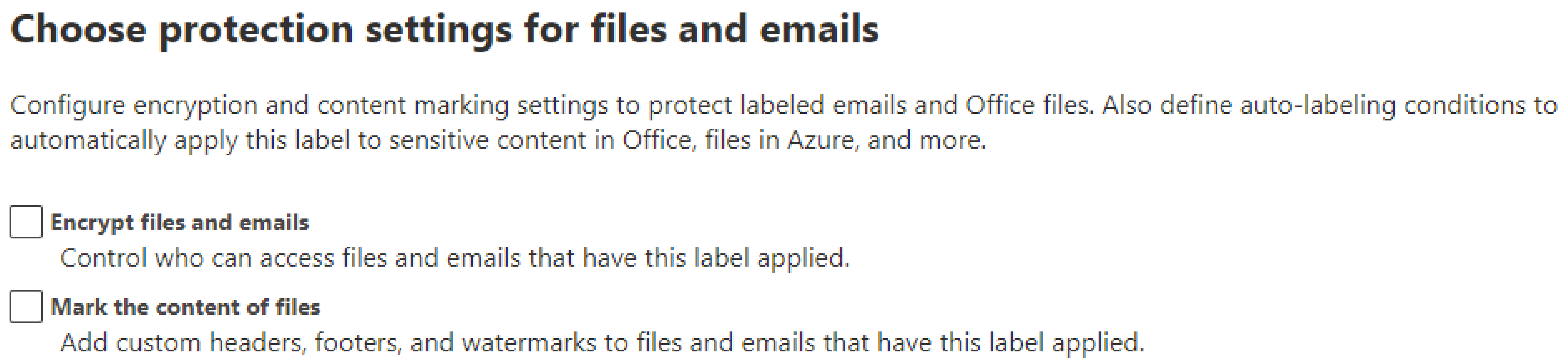
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

ⓘ To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first complete these steps to enable the feature.

□ **Schematized data assets (preview)**

Apply labels to files and schematized data assets in Azure Purview. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

ⓘ To apply this label to Azure Purview assets, you must first turn on labeling for Azure Purview. You can do this from the Labels page. Learn more about labeling for Azure Purview

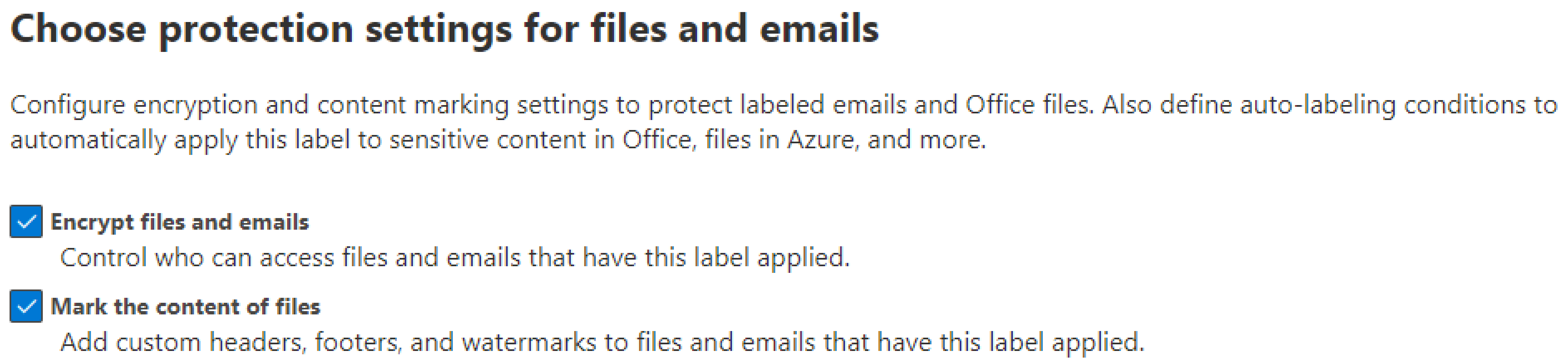


Choose protection settings for files and emails

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

□ **Encrypt files and emails**
Control who can access files and emails that have this label applied.

□ **Mark the content of files**
Add custom headers, footers, and watermarks to files and emails that have this label applied.

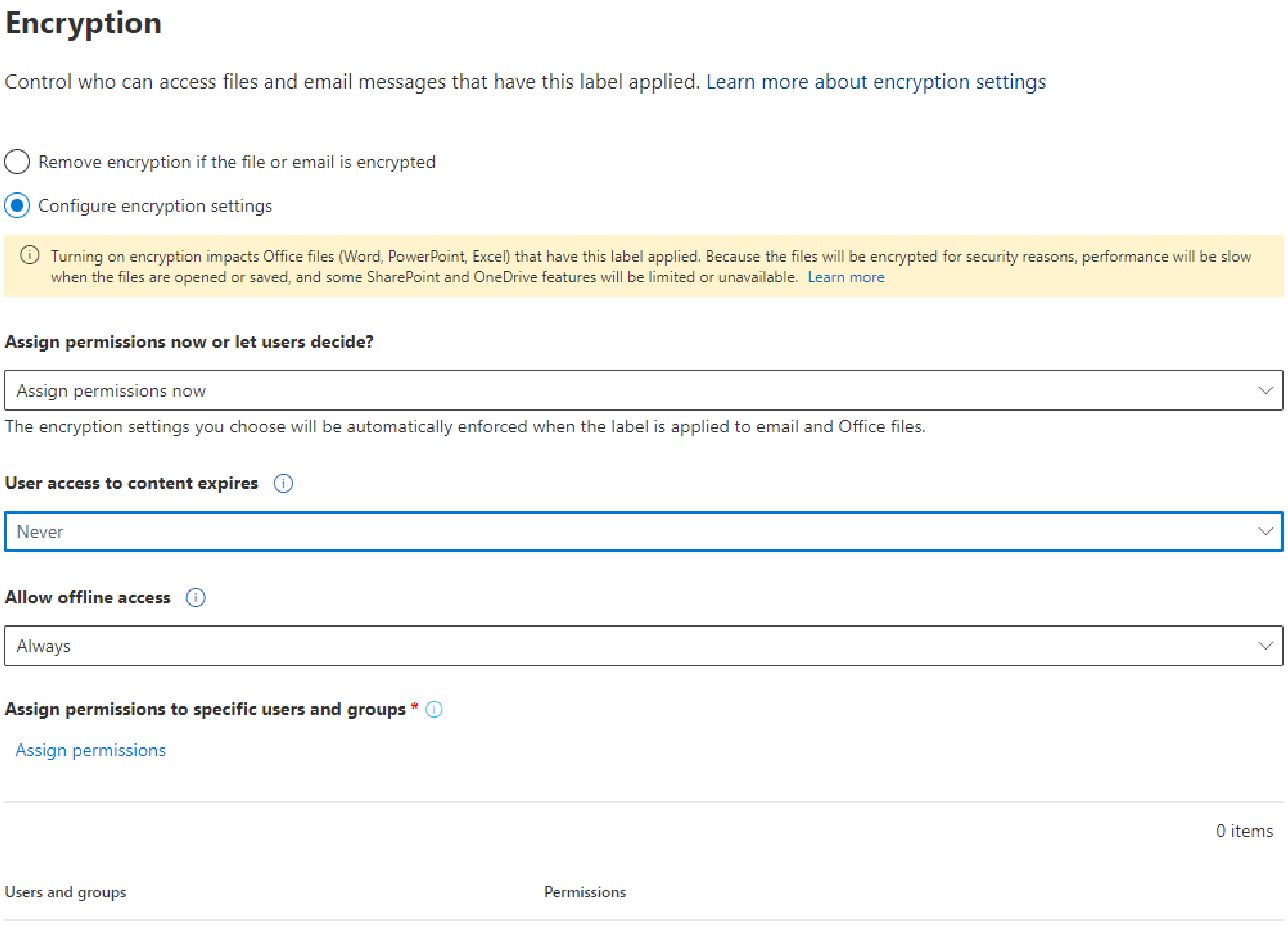


Choose protection settings for files and emails

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

☑ **Encrypt files and emails**
Control who can access files and emails that have this label applied.

☑ **Mark the content of files**
Add custom headers, footers, and watermarks to files and emails that have this label applied.



Encryption

Control who can access files and email messages that have this label applied. Learn more about encryption settings

○ Remove encryption if the file or email is encrypted

● Configure encryption settings

Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires

Never

Allow offline access

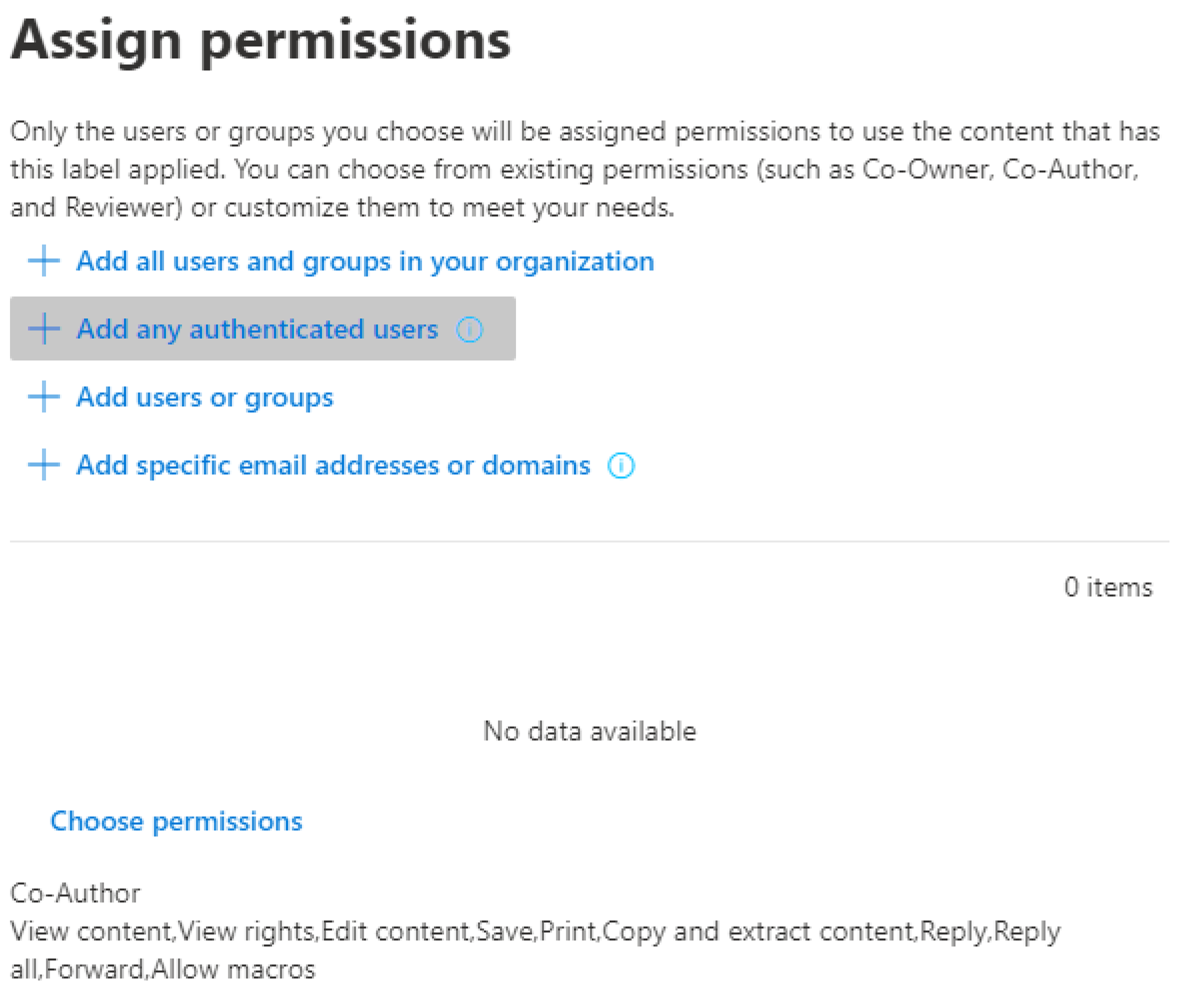
Always

Assign permissions to specific users and groups *

Assign permissions

0 items

Users and groups	Permissions



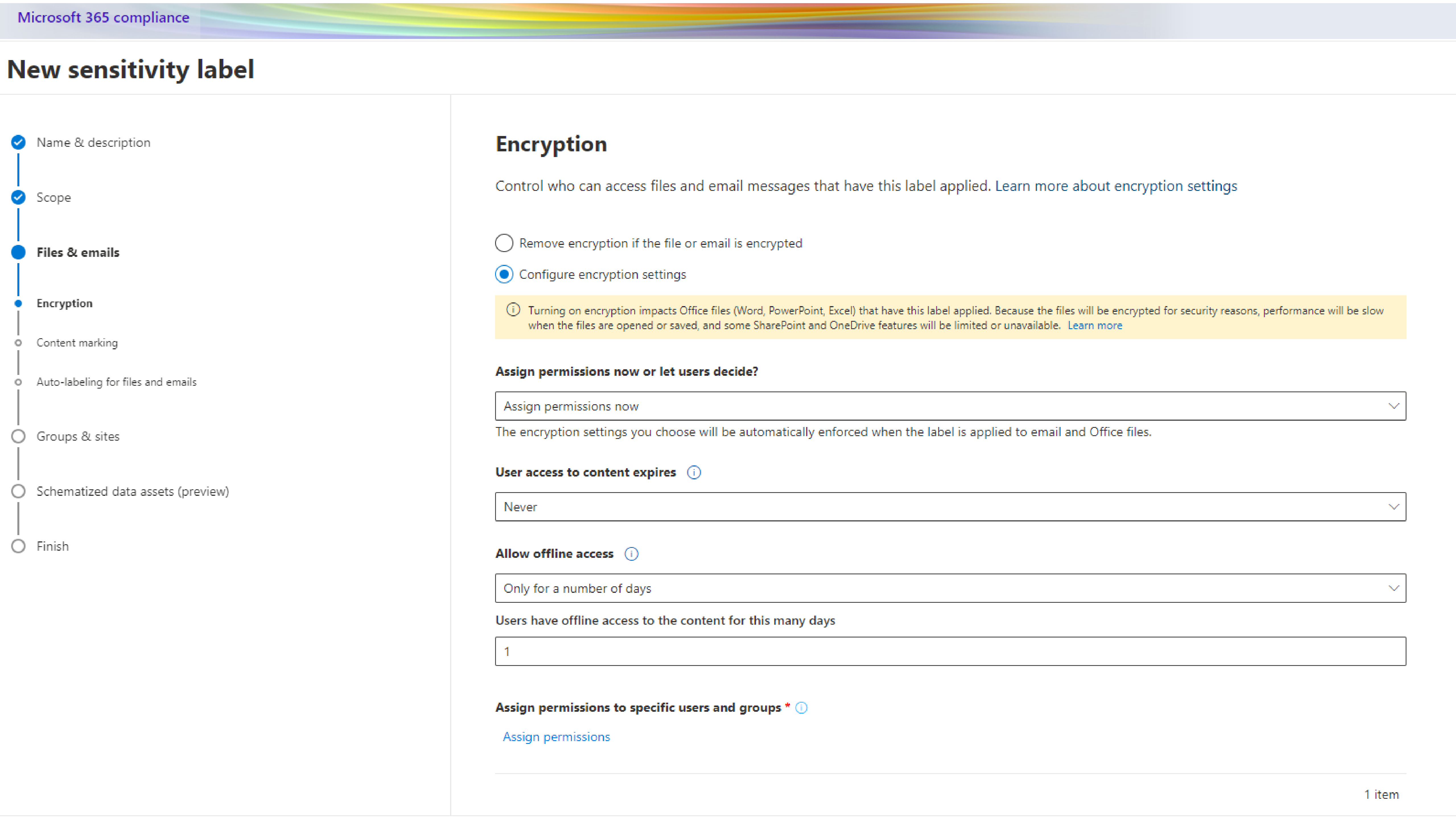
+ Add all users and groups in your organization
+ Add any authenticated users ⓘ
+ Add users or groups
+ Add specific email addresses or domains ⓘ
0 items
Choose permissions

Assign permissions

Only the users or groups you choose will be assigned permissions to use the content that has this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs.

No data available

Co-Author
View content,View rights,Edit content,Save,Print,Copy and extract content,Reply,Reply all,Forward,Allow macros



Microsoft 365 compliance

New sensitivity label

- ✓ Name & description
- ✓ Scope
- ● **Files & emails**
  - ● **Encryption**
  - ○ Content marking
  - ○ Auto-labeling for files and emails
- ○ Groups & sites
- ○ Schematized data assets (preview)
- ○ Finish

Encryption

Control who can access files and email messages that have this label applied. Learn more about encryption settings

○ Remove encryption if the file or email is encrypted

● Configure encryption settings

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

Never

Allow offline access ⓘ

Only for a number of days

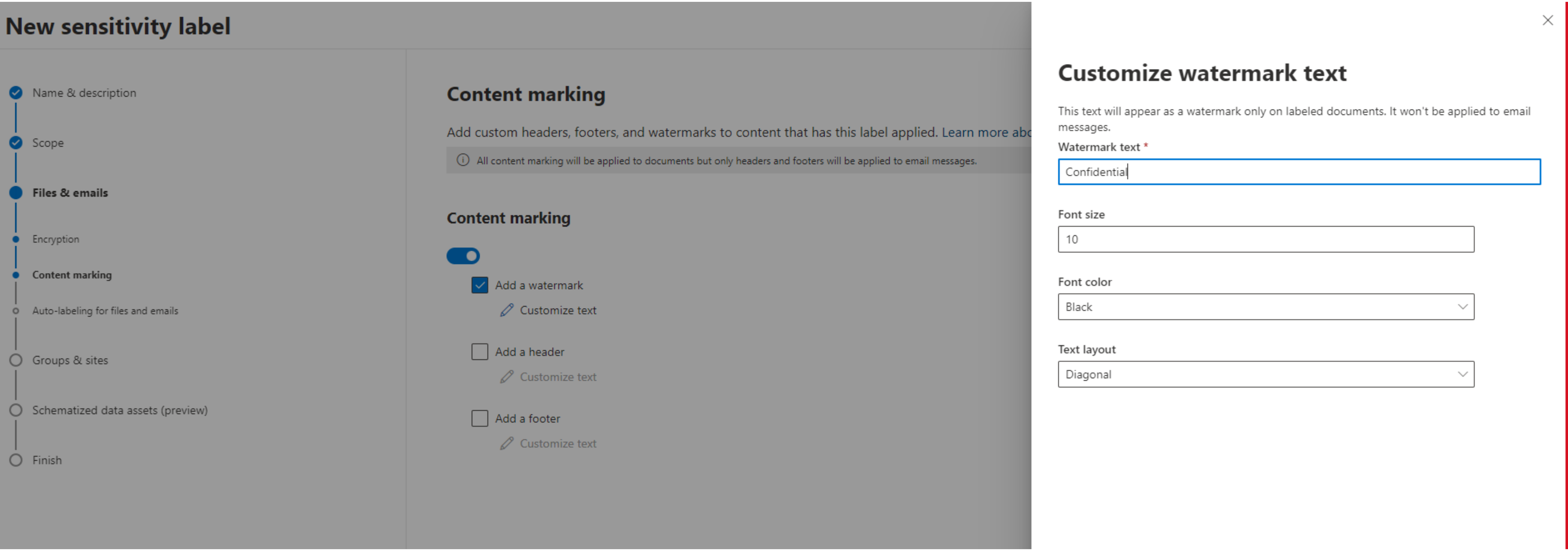
Users have offline access to the content for this many days

1

Assign permissions to specific users and groups * ⓘ

Assign permissions

1 item



New sensitivity label

- ✓ Name & description
- ✓ Scope
- ● **Files & emails**
  - ● Encryption
  - ● **Content marking**
  - ○ Auto-labeling for files and emails
- ○ Groups & sites
- ○ Schematized data assets (preview)
- ○ Finish

Content marking

Add custom headers, footers, and watermarks to content that has this label applied. Learn more abo

ⓘ All content marking will be applied to documents but only headers and footers will be applied to email messages.

Content marking

☑ Add a watermark

Customize text

□ Add a header

Customize text

□ Add a footer

Customize text

Customize watermark text

This text will appear as a watermark only on labeled documents. It won't be applied to email messages.

Watermark text *

Confidential

Font size

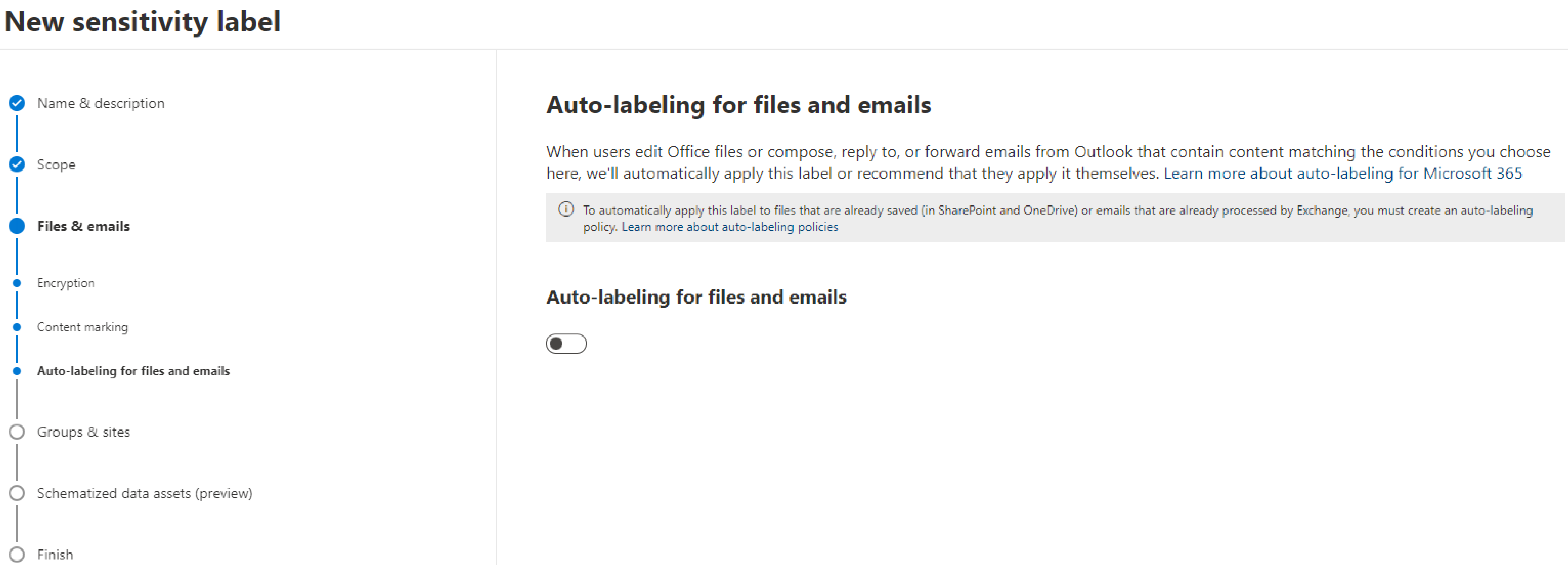
10

Font color

Black

Text layout

Diagonal



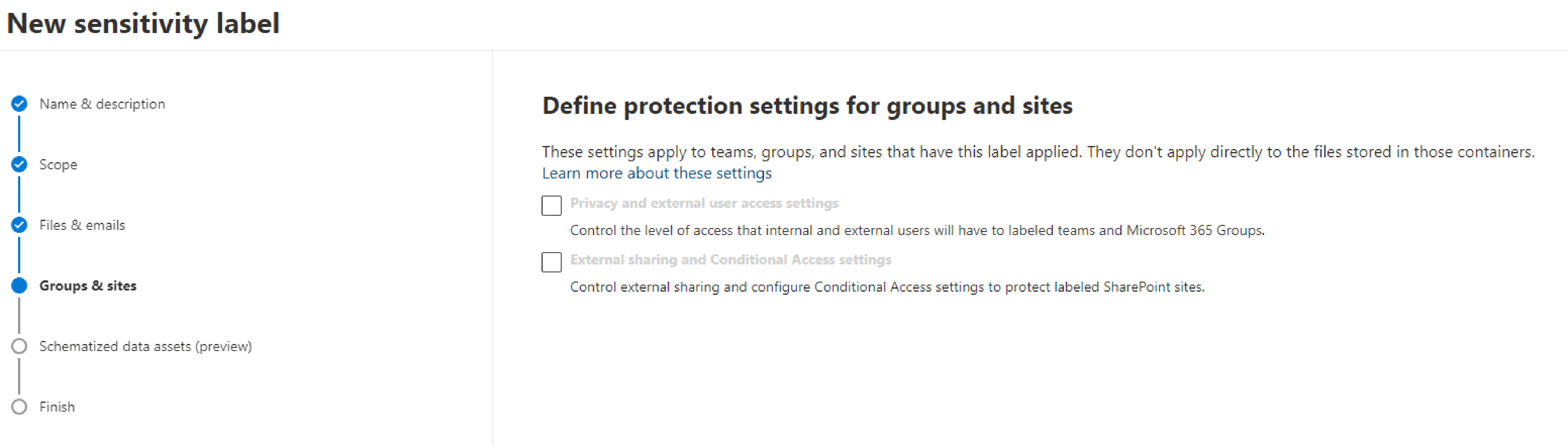
New sensitivity label

Auto-labeling for files and emails

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling for Microsoft 365

ⓘ To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. Learn more about auto-labeling policies

Auto-labeling for files and emails



New sensitivity label

Define protection settings for groups and sites

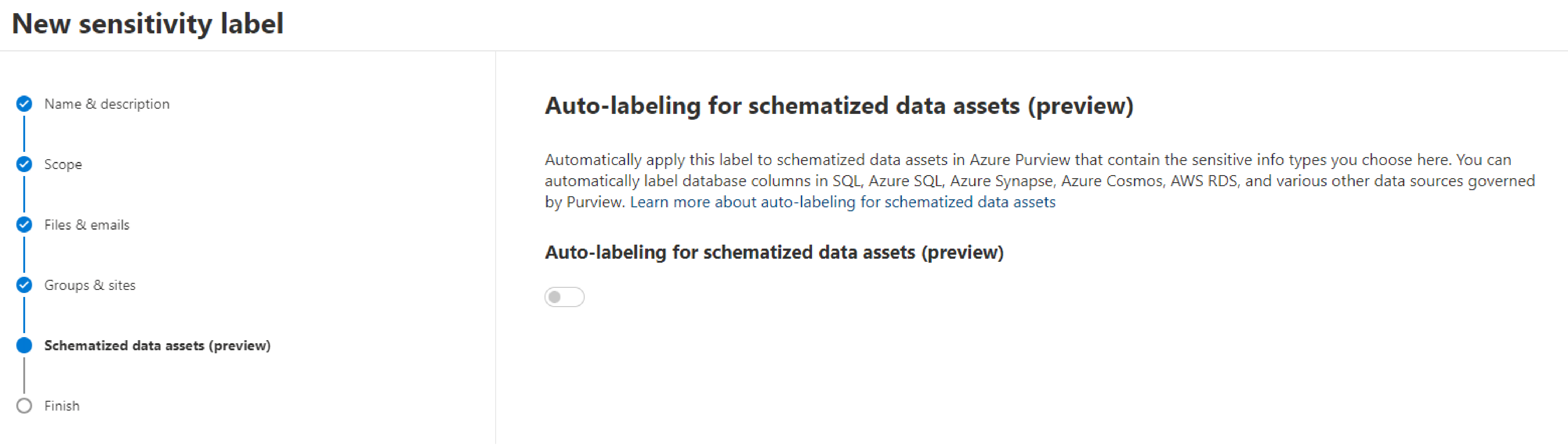
These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers.
Learn more about these settings

□ **Privacy and external user access settings**

Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

□ **External sharing and Conditional Access settings**

Control external sharing and configure Conditional Access settings to protect labeled SharePoint sites.



New sensitivity label

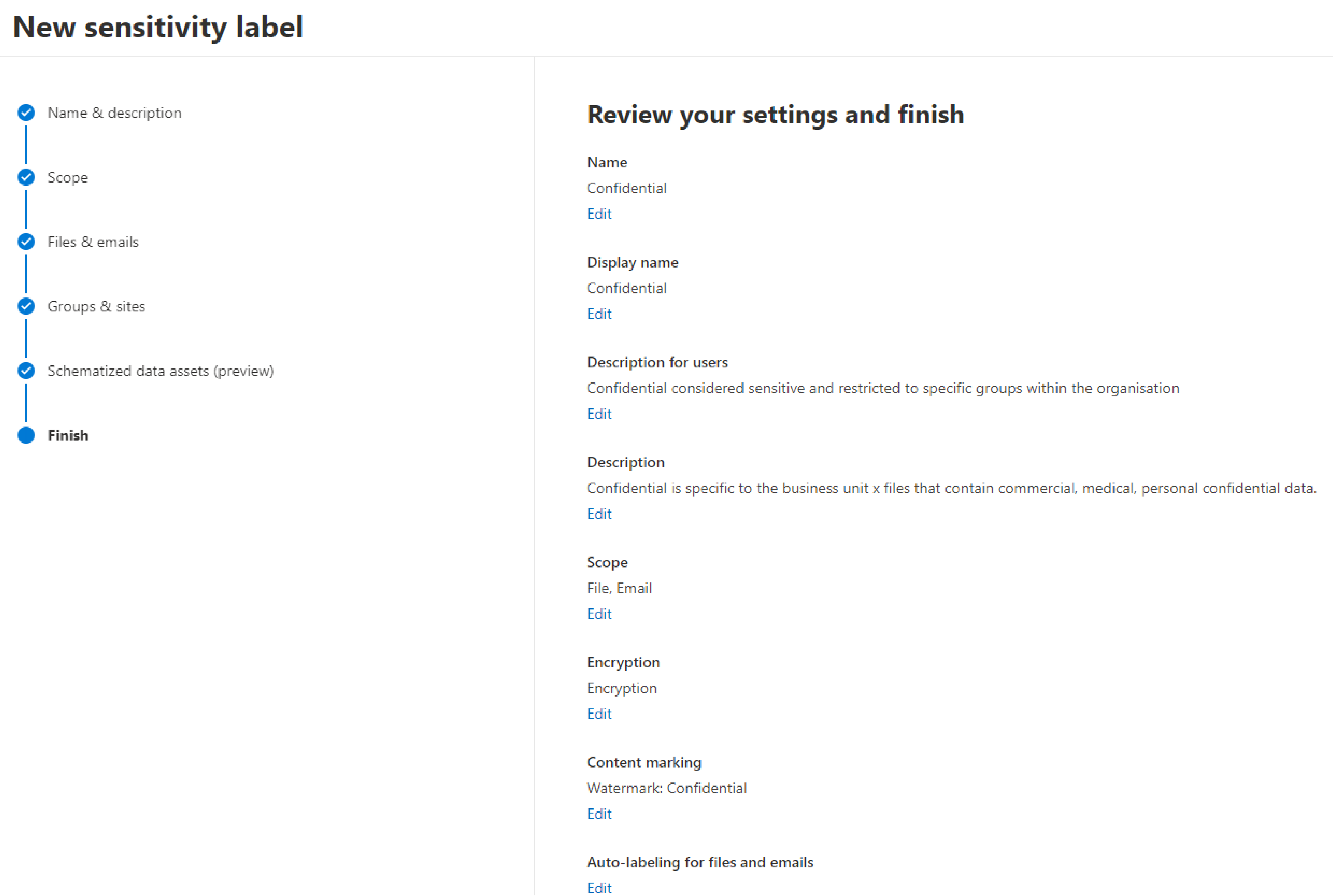
- ✓ Name & description
- ✓ Scope
- ✓ Files & emails
- ✓ Groups & sites
- ● **Schematized data assets (preview)**
- ○ Finish

Auto-labeling for schematized data assets (preview)

Automatically apply this label to schematized data assets in Azure Purview that contain the sensitive info types you choose here. You can automatically label database columns in SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and various other data sources governed by Purview. Learn more about auto-labeling for schematized data assets

Auto-labeling for schematized data assets (preview)

○



New sensitivity label

- ✓ Name & description
- ✓ Scope
- ✓ Files & emails
- ✓ Groups & sites
- ✓ Schematized data assets (preview)
- ● **Finish**

Review your settings and finish

Name

Confidential

Edit

Display name

Confidential

Edit

Description for users

Confidential considered sensitive and restricted to specific groups within the organisation

Edit

Description

Confidential is specific to the business unit x files that contain commercial, medical, personal confidential data.

Edit

Scope

File, Email

Edit

Encryption

Encryption

Edit

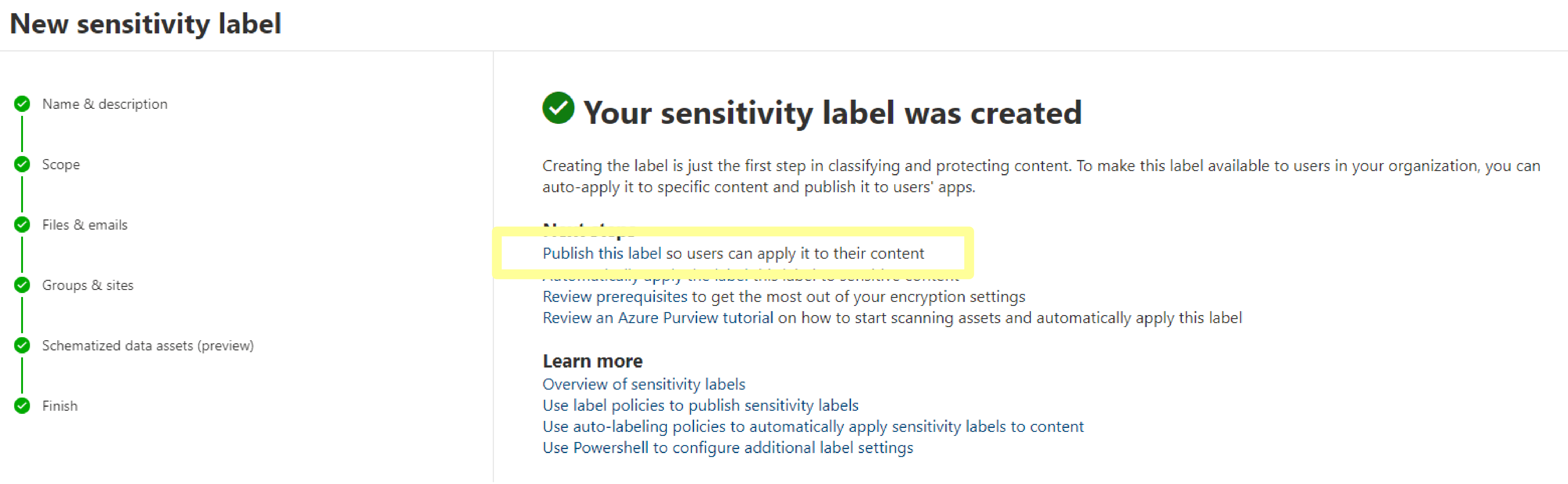
Content marking

Watermark: Confidential

Edit

Auto-labeling for files and emails

Edit



New sensitivity label

- ✓ Name & description
- ✓ Scope
- ✓ Files & emails
- ✓ Groups & sites
- ✓ Schematized data assets (preview)
- ✓ Finish

✓ Your sensitivity label was created

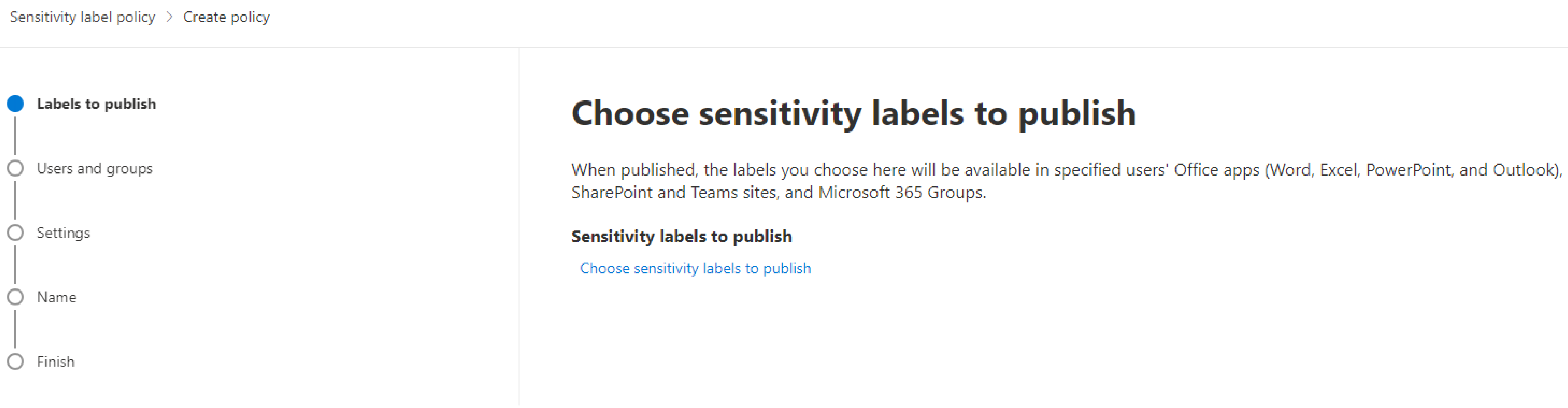
Creating the label is just the first step in classifying and protecting content. To make this label available to users in your organization, you can auto-apply it to specific content and publish it to users' apps.

Next steps

Publish this label so users can apply it to their content
Automatically apply the label this label to sensitive content
Review prerequisites to get the most out of your encryption settings
Review an Azure Purview tutorial on how to start scanning assets and automatically apply this label

Learn more

Overview of sensitivity labels
Use label policies to publish sensitivity labels
Use auto-labeling policies to automatically apply sensitivity labels to content
Use Powershell to configure additional label settings



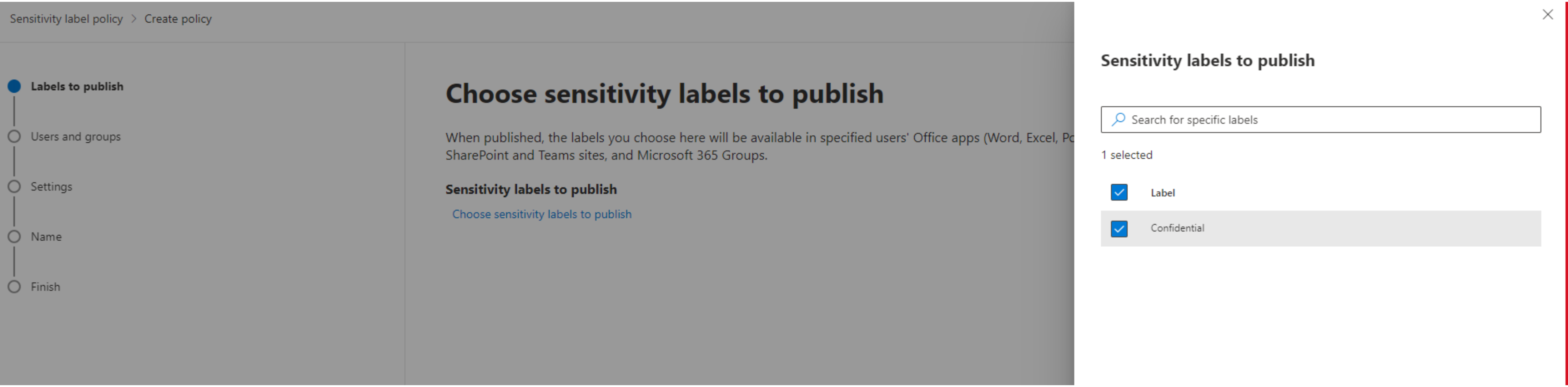
Sensitivity label policy > Create policy
Labels to publish
Users and groups
Settings
Name
Finish

Choose sensitivity labels to publish

When published, the labels you choose here will be available in specified users' Office apps (Word, Excel, PowerPoint, and Outlook), SharePoint and Teams sites, and Microsoft 365 Groups.

Sensitivity labels to publish

Choose sensitivity labels to publish



Sensitivity label policy > Create policy
● Labels to publish
○ Users and groups
○ Settings
○ Name
○ Finish

Choose sensitivity labels to publish

When published, the labels you choose here will be available in specified users' Office apps (Word, Excel, Po
SharePoint and Teams sites, and Microsoft 365 Groups.

Sensitivity labels to publish

Choose sensitivity labels to publish

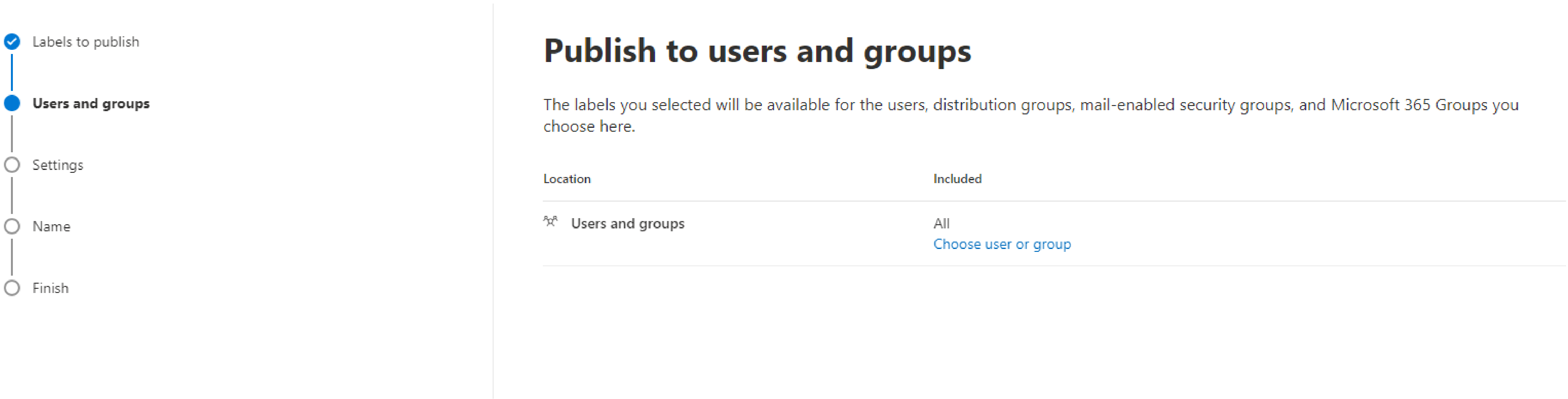
Sensitivity labels to publish

Search for specific labels

1 selected

☑ Label

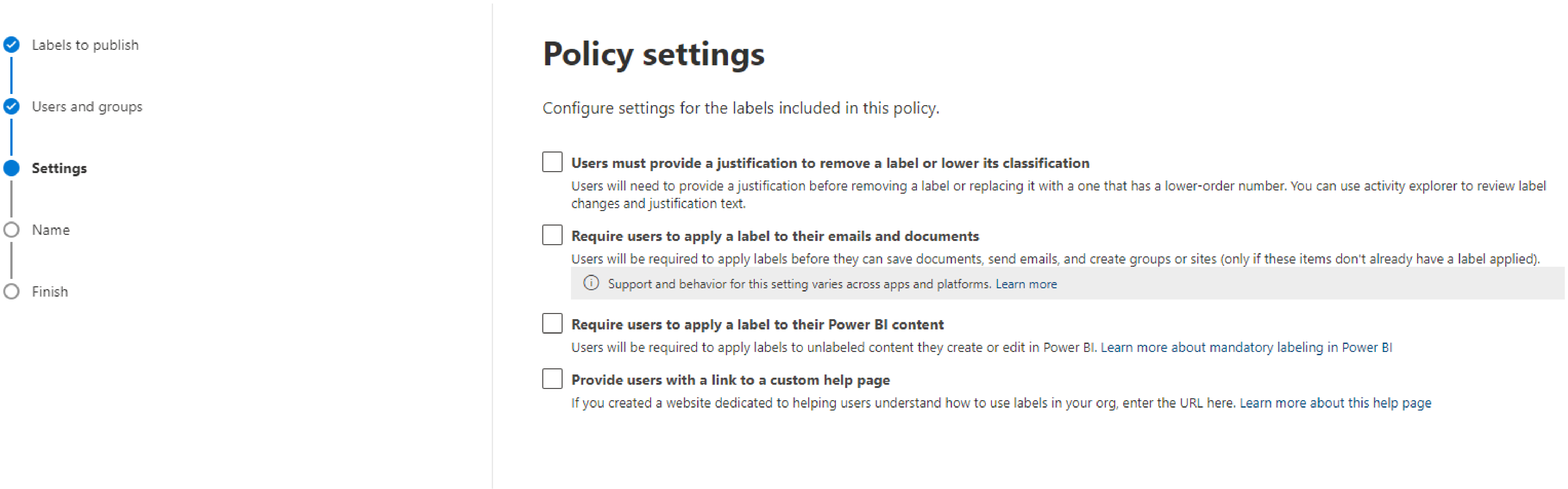
☑ Confidential



Publish to users and groups

The labels you selected will be available for the users, distribution groups, mail-enabled security groups, and Microsoft 365 Groups you choose here.

Location	Included
Users and groups	All Choose user or group



Policy settings

Configure settings for the labels included in this policy.

□ **Users must provide a justification to remove a label or lower its classification**

Users will need to provide a justification before removing a label or replacing it with a one that has a lower-order number. You can use activity explorer to review label changes and justification text.

□ **Require users to apply a label to their emails and documents**

Users will be required to apply labels before they can save documents, send emails, and create groups or sites (only if these items don't already have a label applied).

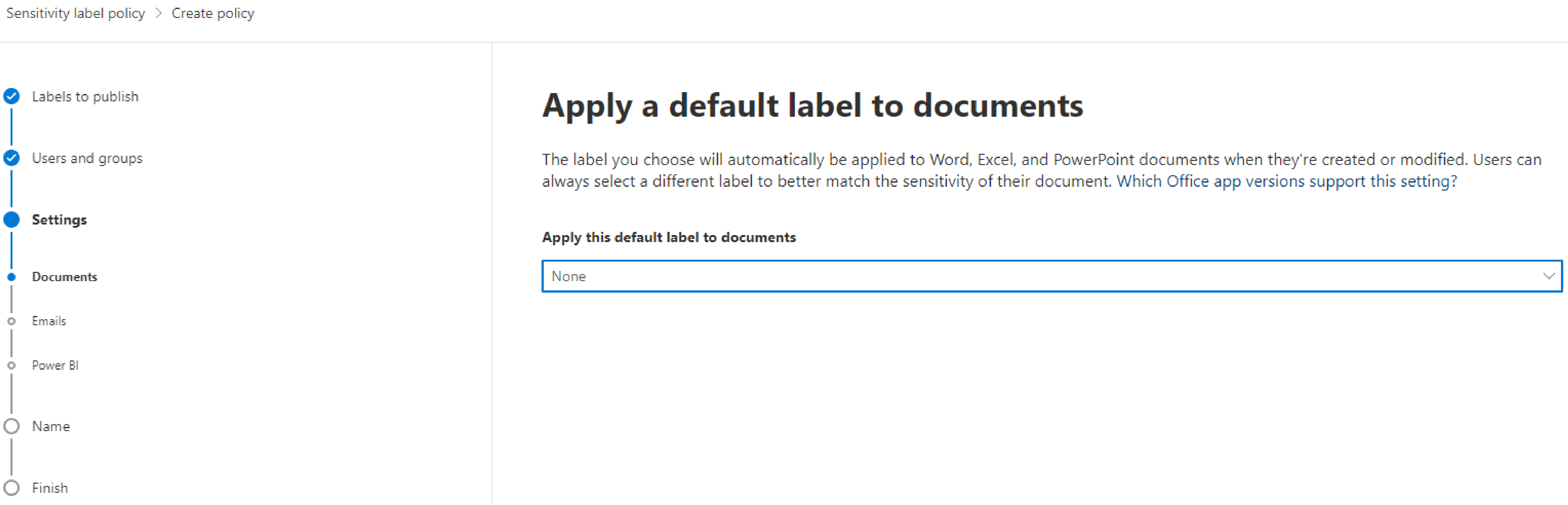
ⓘ Support and behavior for this setting varies across apps and platforms. Learn more

□ **Require users to apply a label to their Power BI content**

Users will be required to apply labels to unlabeled content they create or edit in Power BI. Learn more about mandatory labeling in Power BI

□ **Provide users with a link to a custom help page**

If you created a website dedicated to helping users understand how to use labels in your org, enter the URL here. Learn more about this help page

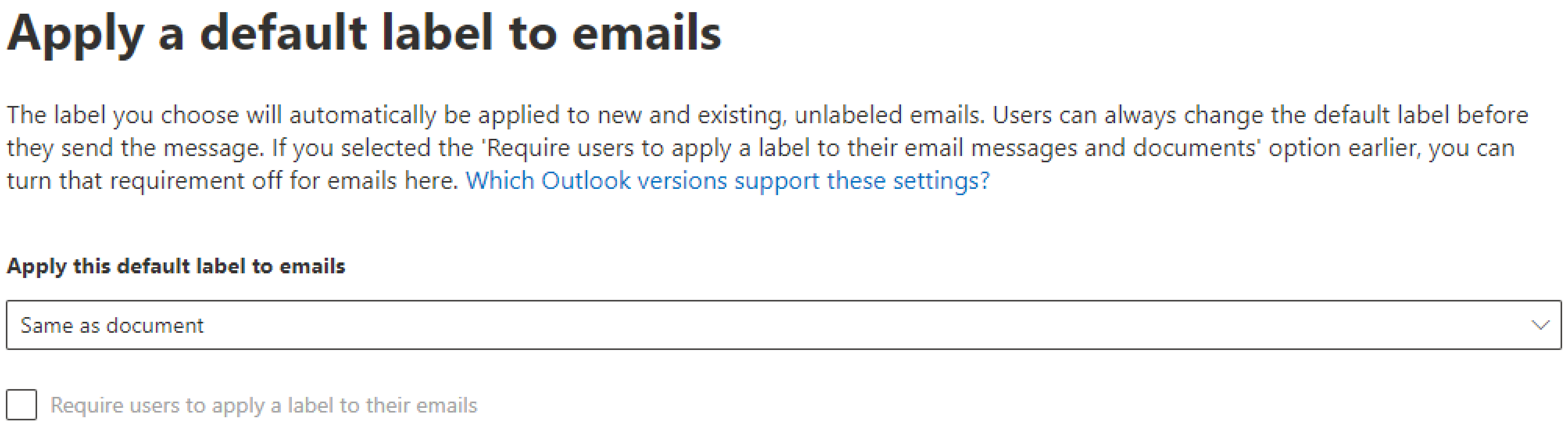


Apply a default label to documents

The label you choose will automatically be applied to Word, Excel, and PowerPoint documents when they're created or modified. Users can always select a different label to better match the sensitivity of their document. Which Office app versions support this setting?

Apply this default label to documents

None



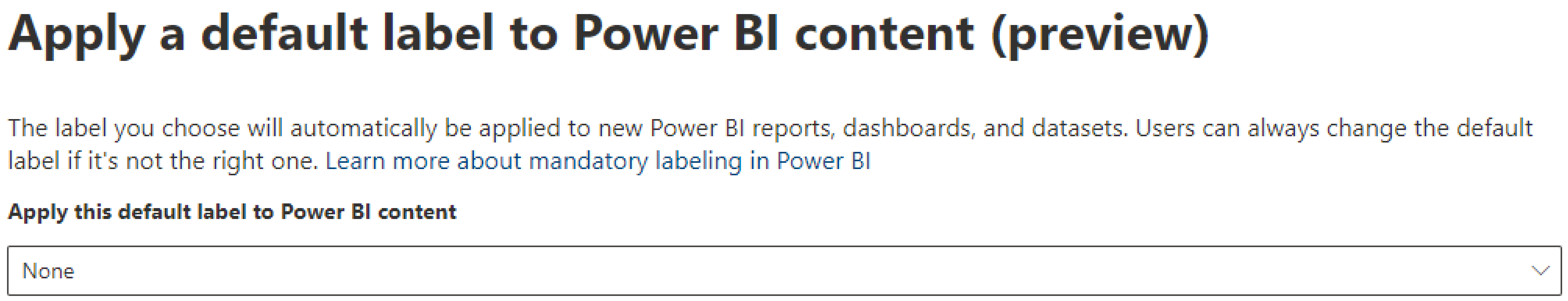
Apply a default label to emails

The label you choose will automatically be applied to new and existing, unlabeled emails. Users can always change the default label before they send the message. If you selected the 'Require users to apply a label to their email messages and documents' option earlier, you can turn that requirement off for emails here. Which Outlook versions support these settings?

Apply this default label to emails

Same as document

□ Require users to apply a label to their emails

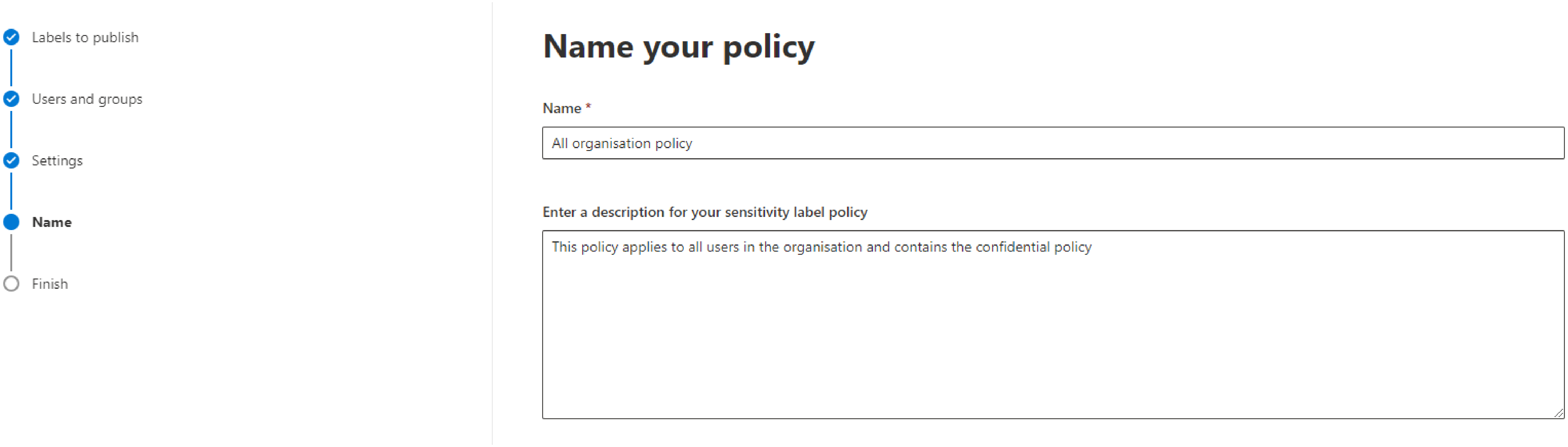


Apply a default label to Power BI content (preview)

The label you choose will automatically be applied to new Power BI reports, dashboards, and datasets. Users can always change the default label if it's not the right one. Learn more about mandatory labeling in Power BI

Apply this default label to Power BI content

None



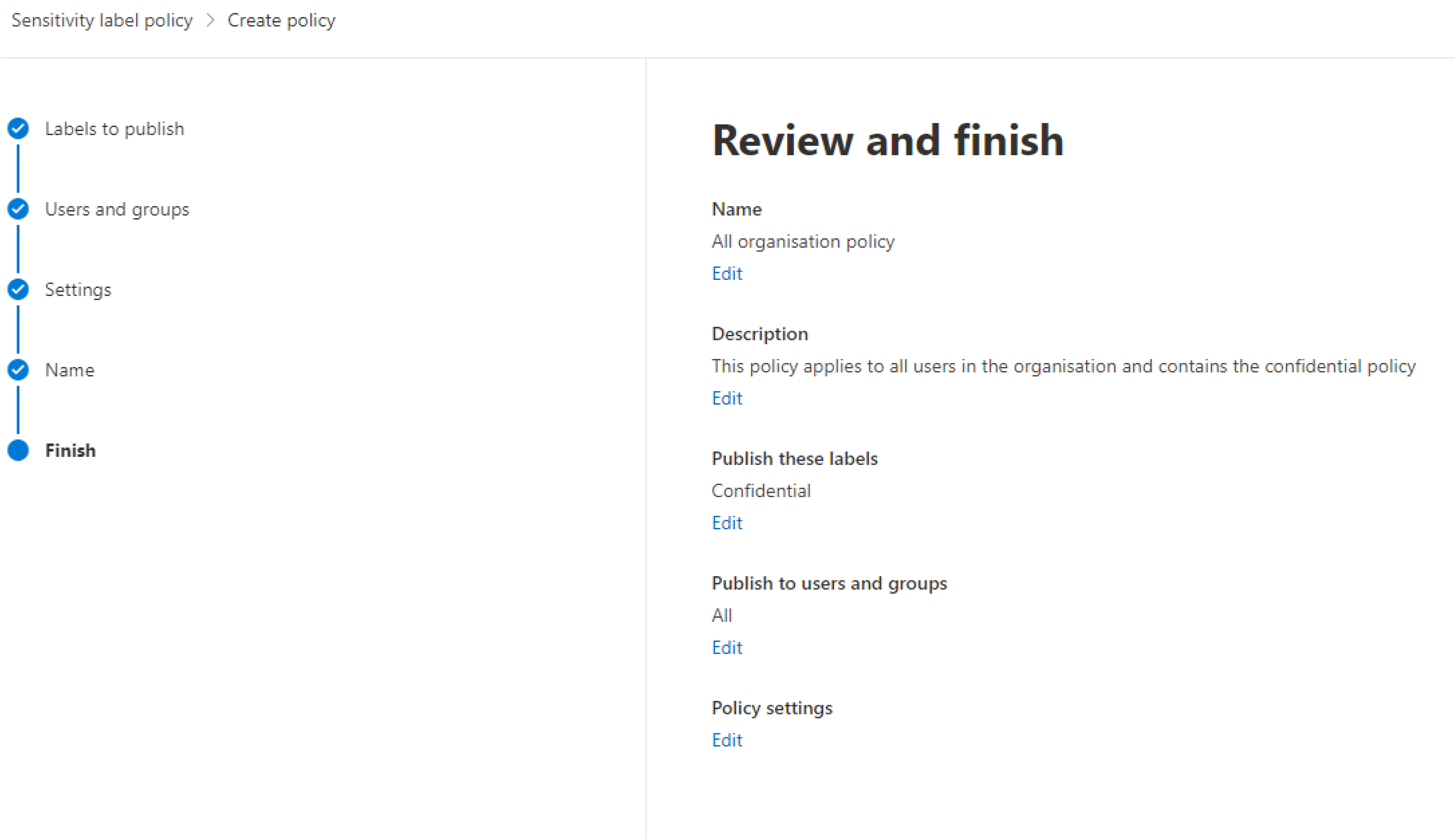
Name your policy

Name *

All organisation policy

Enter a description for your sensitivity label policy

This policy applies to all users in the organisation and contains the confidential policy



Sensitivity label policy > Create policy

- ✓ Labels to publish
- ✓ Users and groups
- ✓ Settings
- ✓ Name
- ● **Finish**

Review and finish

Name

All organisation policy

Edit

Description

This policy applies to all users in the organisation and contains the confidential policy

Edit

Publish these labels

Confidential

Edit

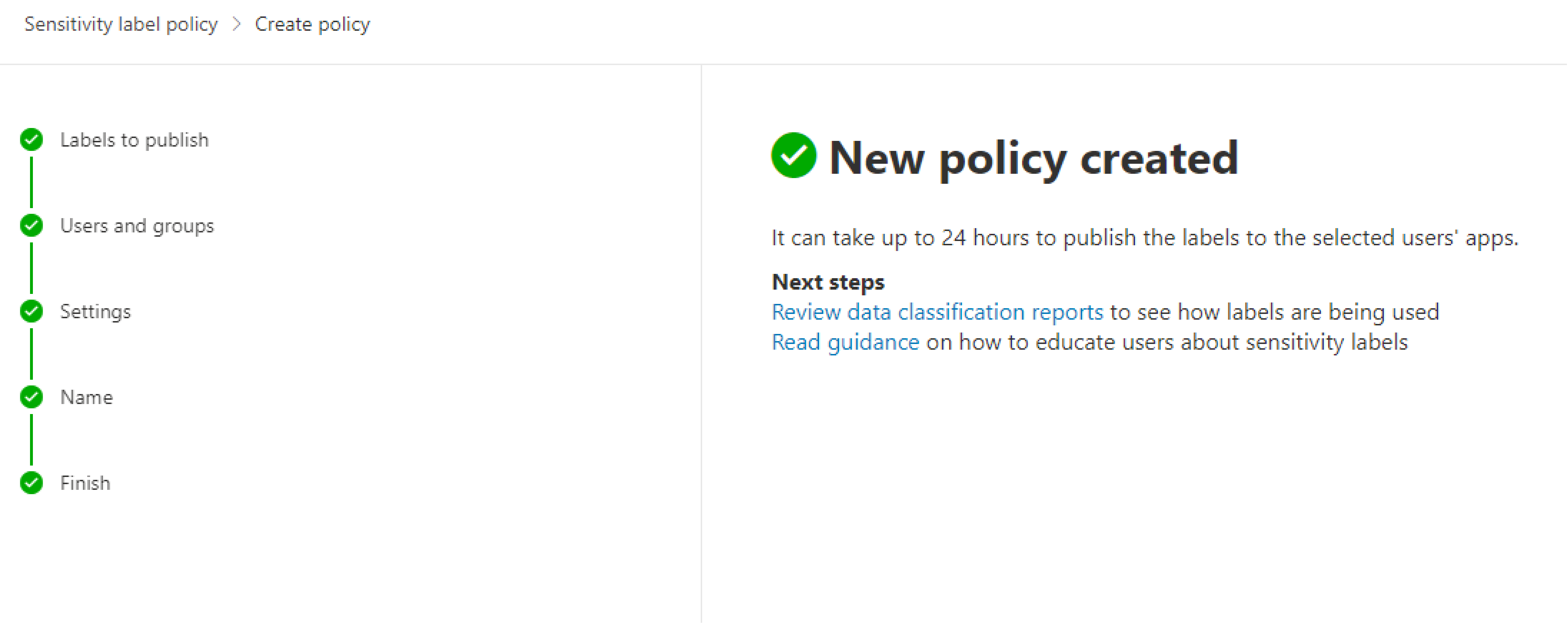
Publish to users and groups

All

Edit

Policy settings

Edit



✓ New policy created

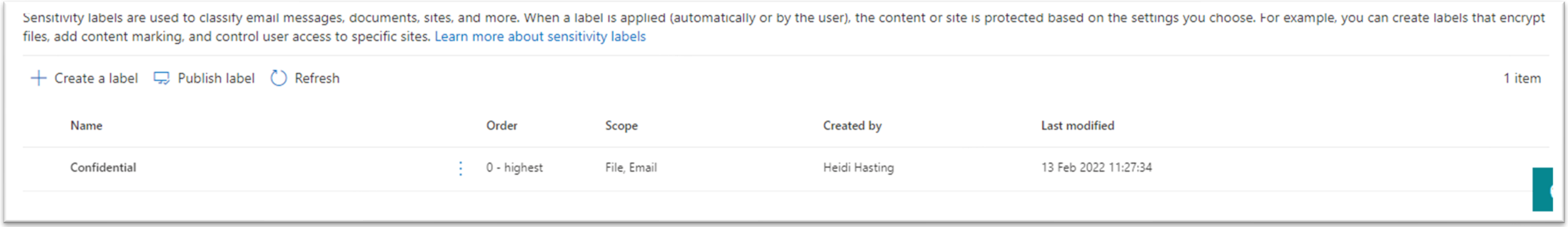
It can take up to 24 hours to publish the labels to the selected users' apps.

Next steps

Review data classification reports to see how labels are being used

Read guidance on how to educate users about sensitivity labels

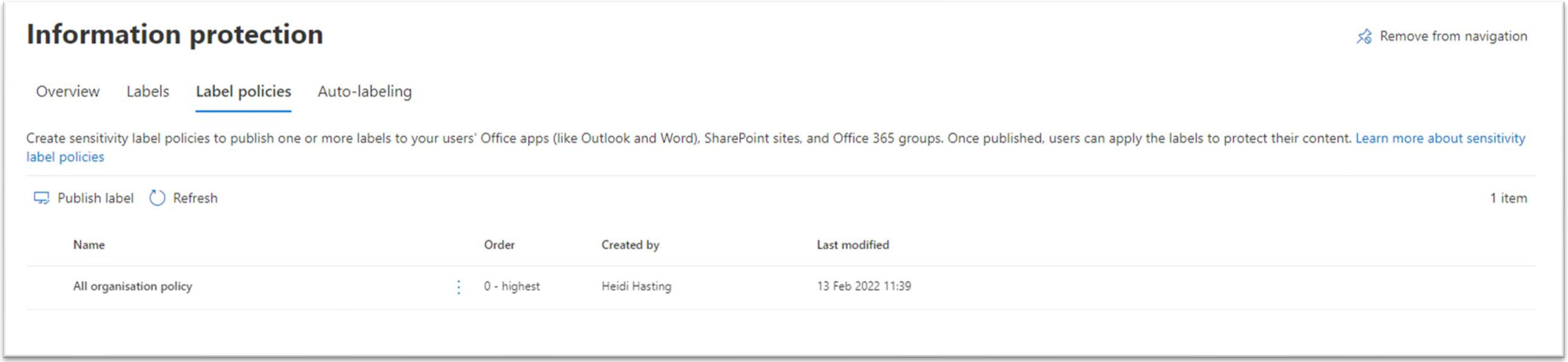
Label



Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

Name	Order	Scope	Created by	Last modified
Confidential	0 - highest	File, Email	Heidi Hasting	13 Feb 2022 11:27:34

Policy

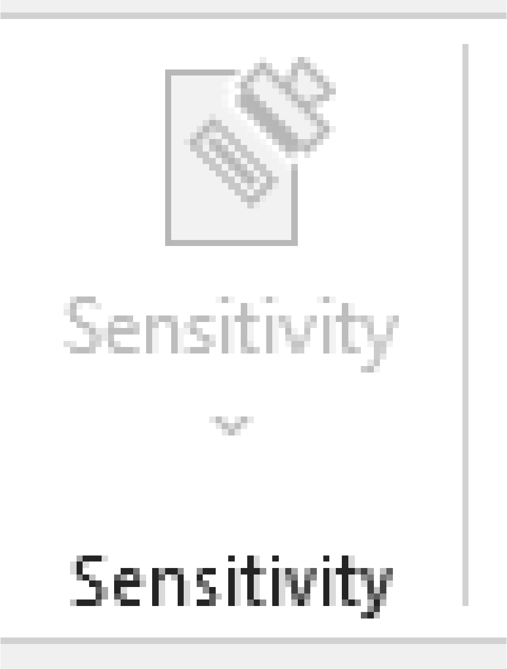


Information protection

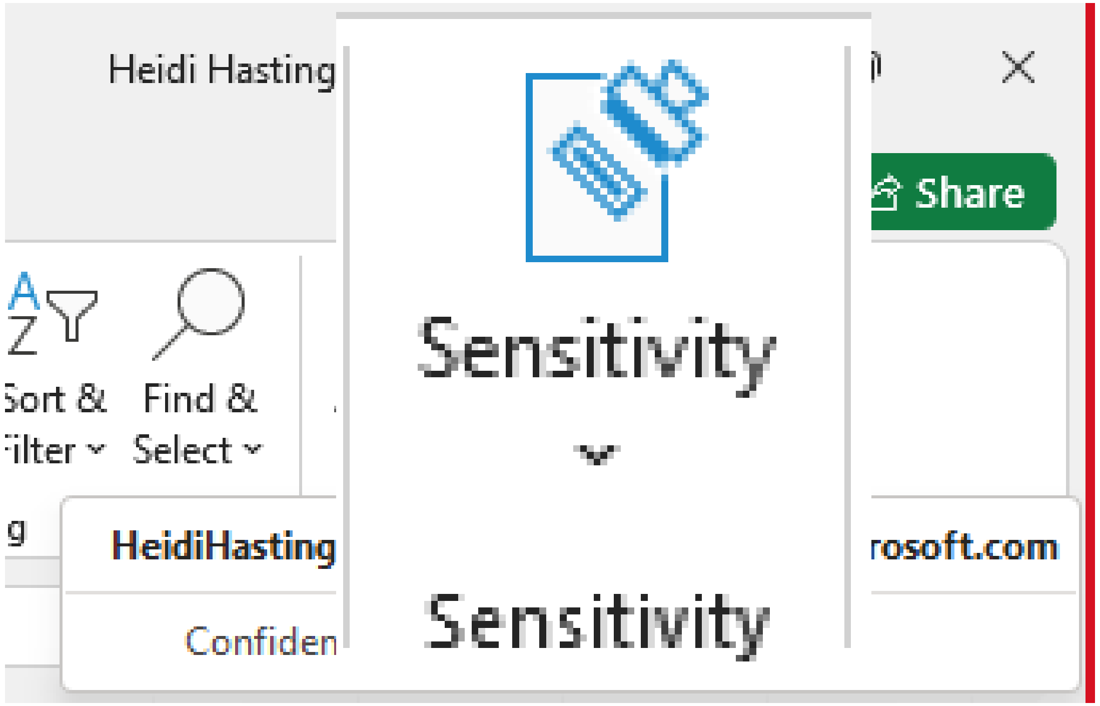
Create sensitivity label policies to publish one or more labels to your users' Office apps (like Outlook and Word), SharePoint sites, and Office 365 groups. Once published, users can apply the labels to protect their content. Learn more about sensitivity label policies

Name	Order	Created by	Last modified
All organisation policy	0 - highest	Heidi Hasting	13 Feb 2022 11:39

Excel *(store in blob storage)*

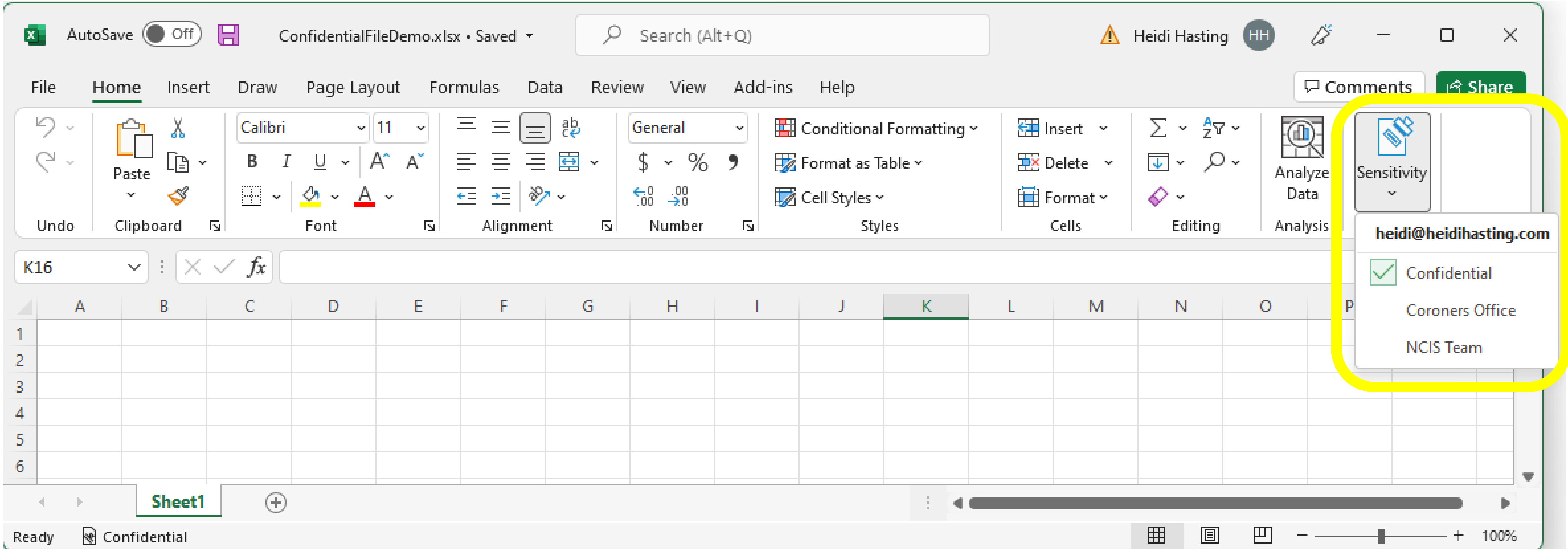


Tenant without sensitivity labels setup
OR not signed in

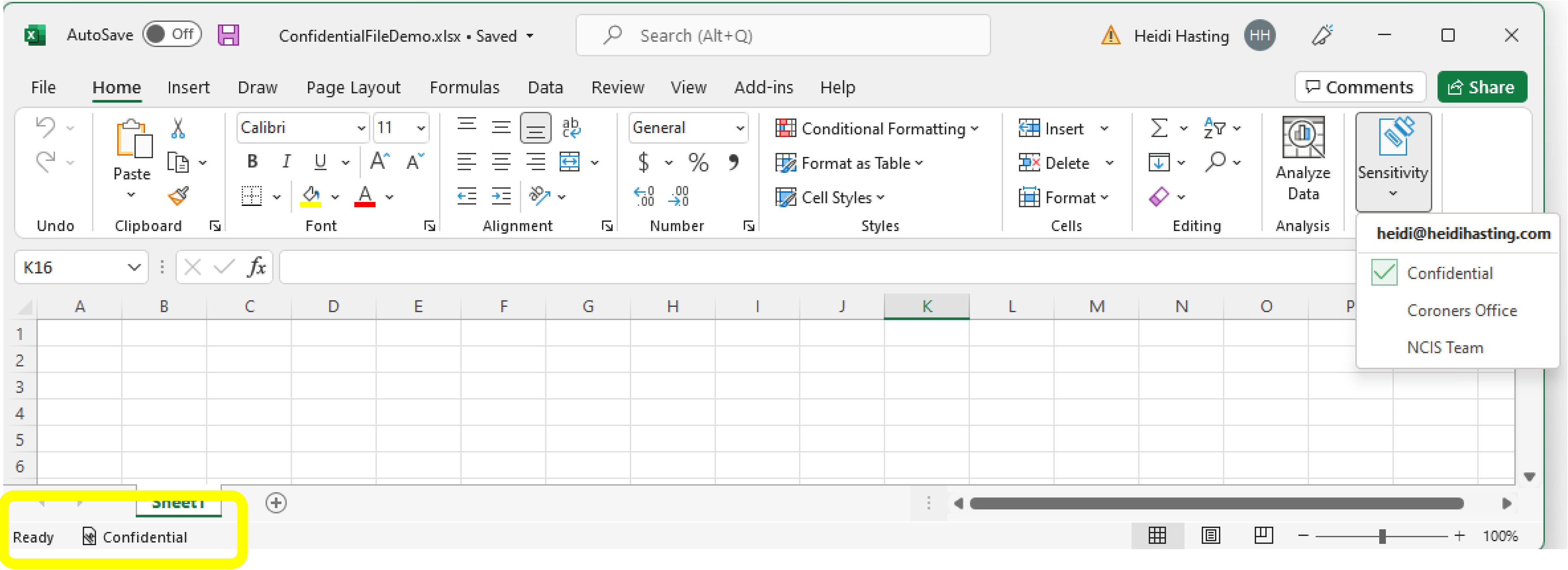


Tenant with sensitivity labels setup

Apply sensitivity label



Apply sensitivity label



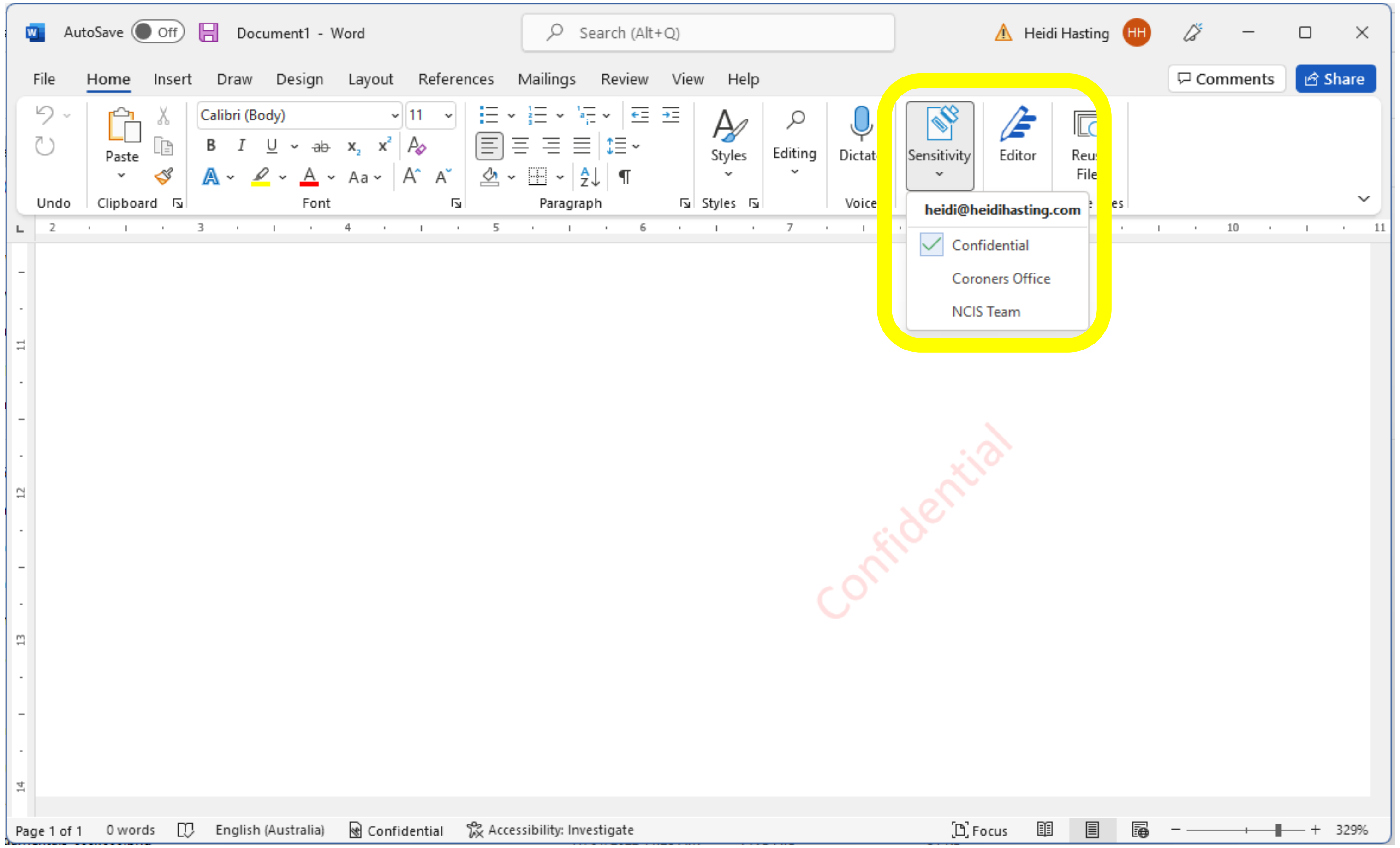
heidi@heidihasting.com

✓ Confidential

Coroners Office

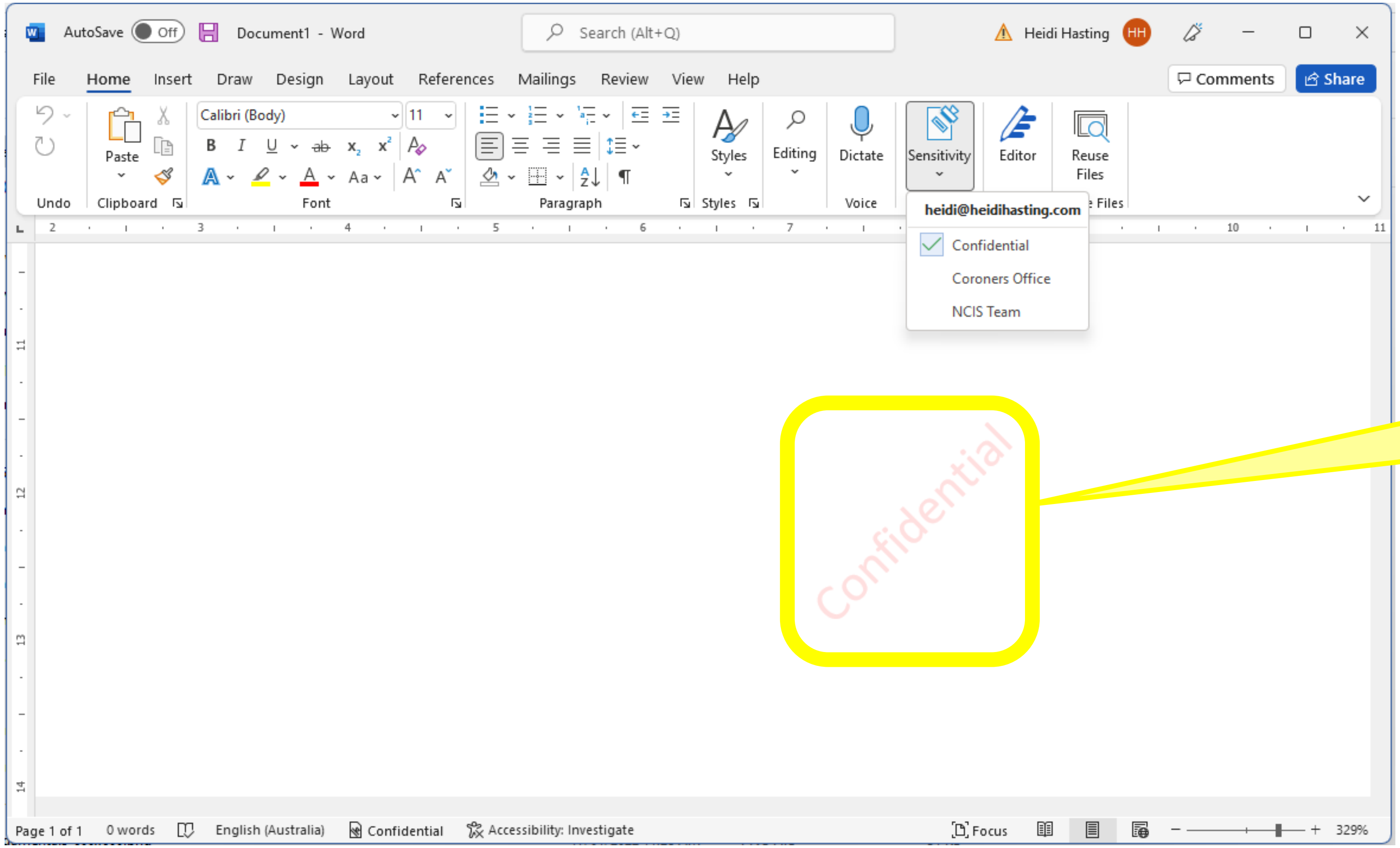
NCIS Team

Word



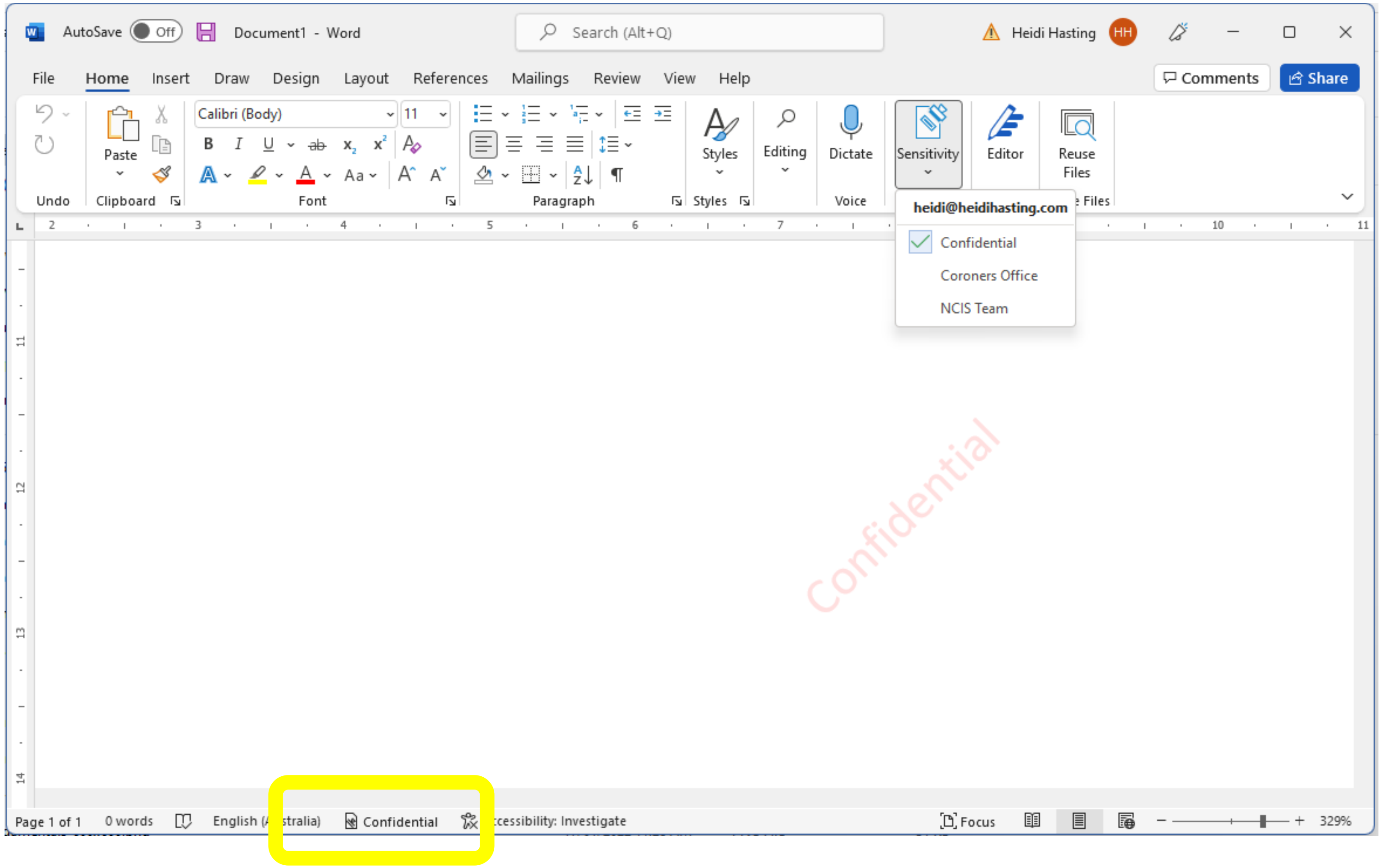
AutoSave Off
Document1 - Word
Search (Alt+Q)
Heidi Hasting HH
File
Home
Insert
Draw
Design
Layout
References
Mailings
Review
View
Help
Comments
Share
Undo
Paste
Clipboard
Calibri (Body)
11
Font
Paragraph
Styles
Editing
Dictat
Voice
Sensitivity
Editor
Reu
File
heidi@heidihasting.com
Confidential
Coroners Office
NCIS Team
Confidential
Page 1 of 1
0 words
English (Australia)
Confidential
Accessibility: Investigate
Focus
329%

Word



Watermark applied

Word

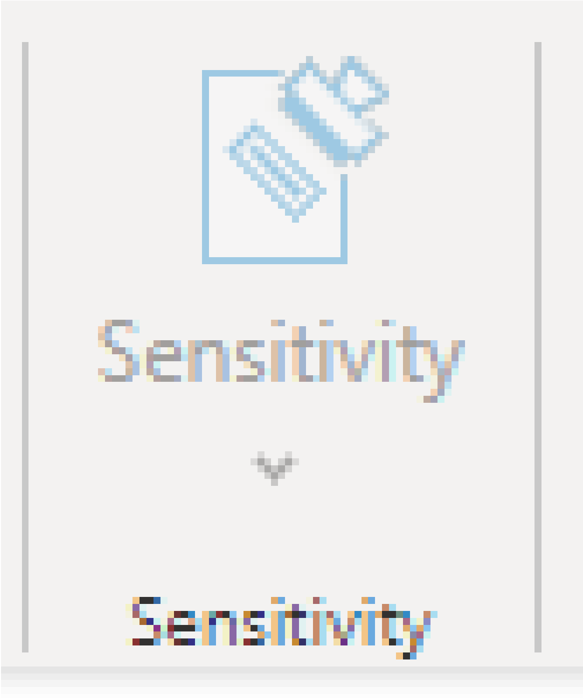

AutoSave Off
Document1 - Word
Search (Alt+Q)
Heidi Hasting HH
File
Home
Insert
Draw
Design
Layout
References
Mailings
Review
View
Help
Comments
Share
Undo
Paste
Clipboard
Calibri (Body)
11
Font
Paragraph
Styles
Editing
Dictate
Voice
Sensitivity
Editor
Reuse Files
heidi@heidihasting.com
✓ Confidential
Coroners Office
NCIS Team
Confidential
Page 1 of 1
0 words
English (Australia)
Confidential
Accessibility: Investigate
Focus
329%

Power BI
(Desktop/Service) – NOT Power BI Report Server

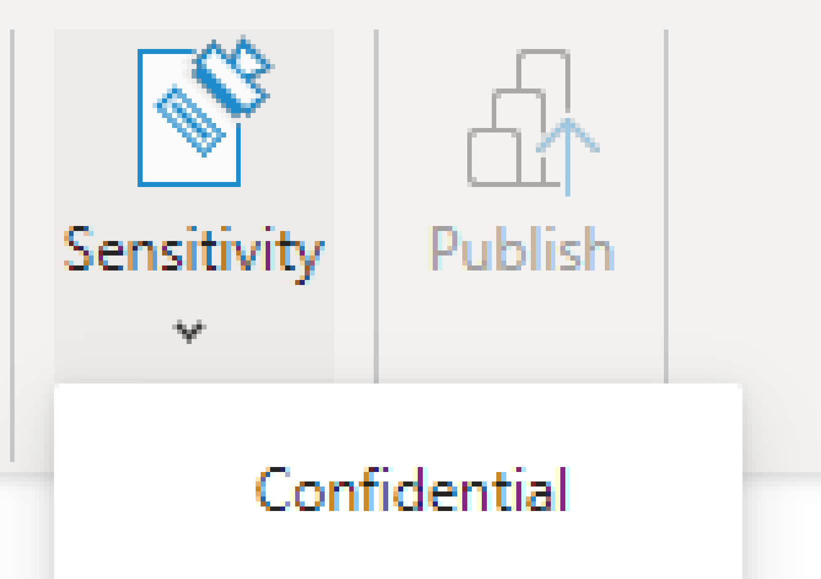
- Dashboards
- Reports
- Datamarts
- Datasets
- Dataflows
- Paginated reports*
- NOT workbooks

** apply via Power BI Service*

Power BI Desktop

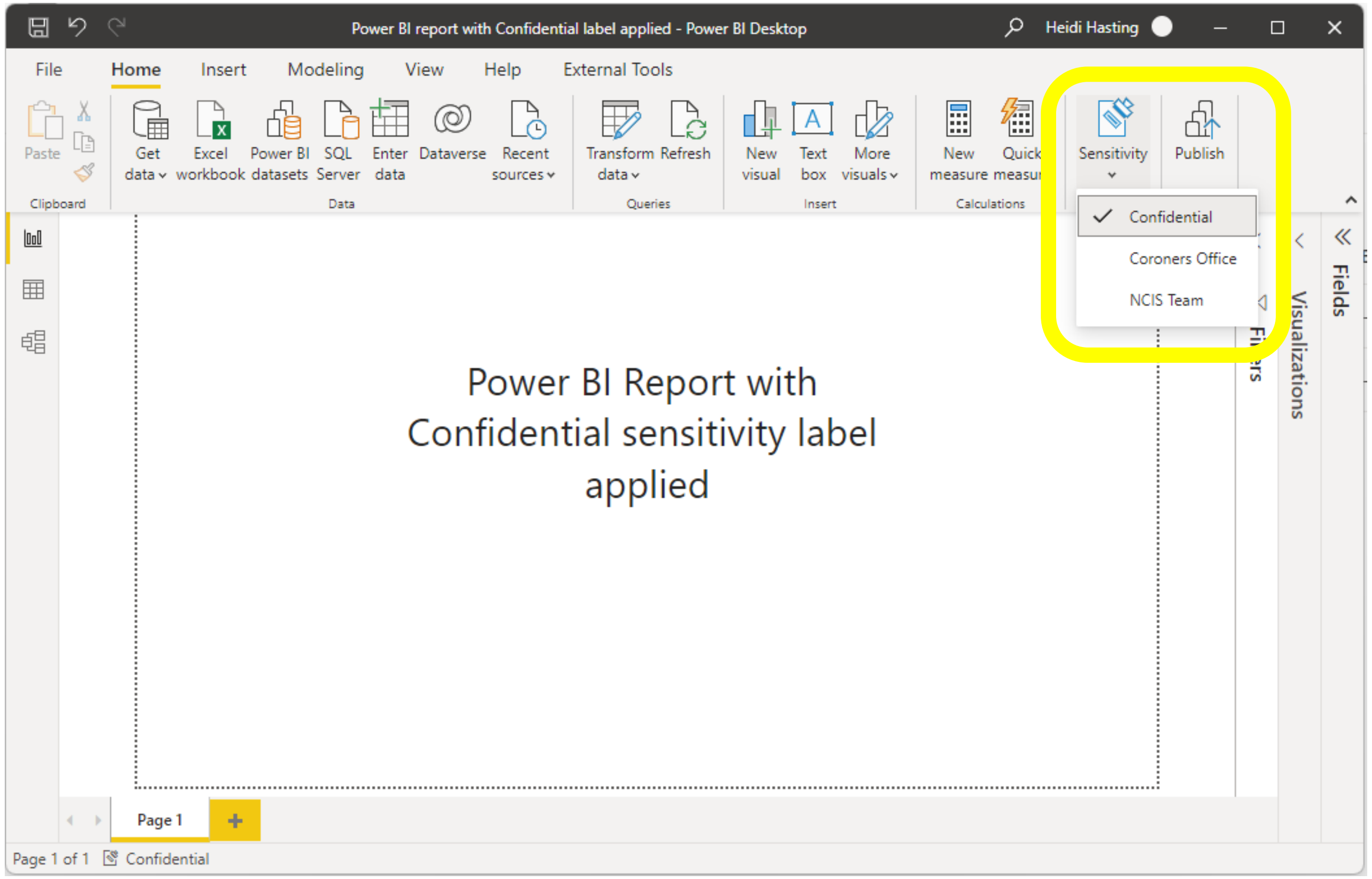


Tenant without sensitivity labels setup
Or not logged in



Tenant with sensitivity labels setup

Power BI

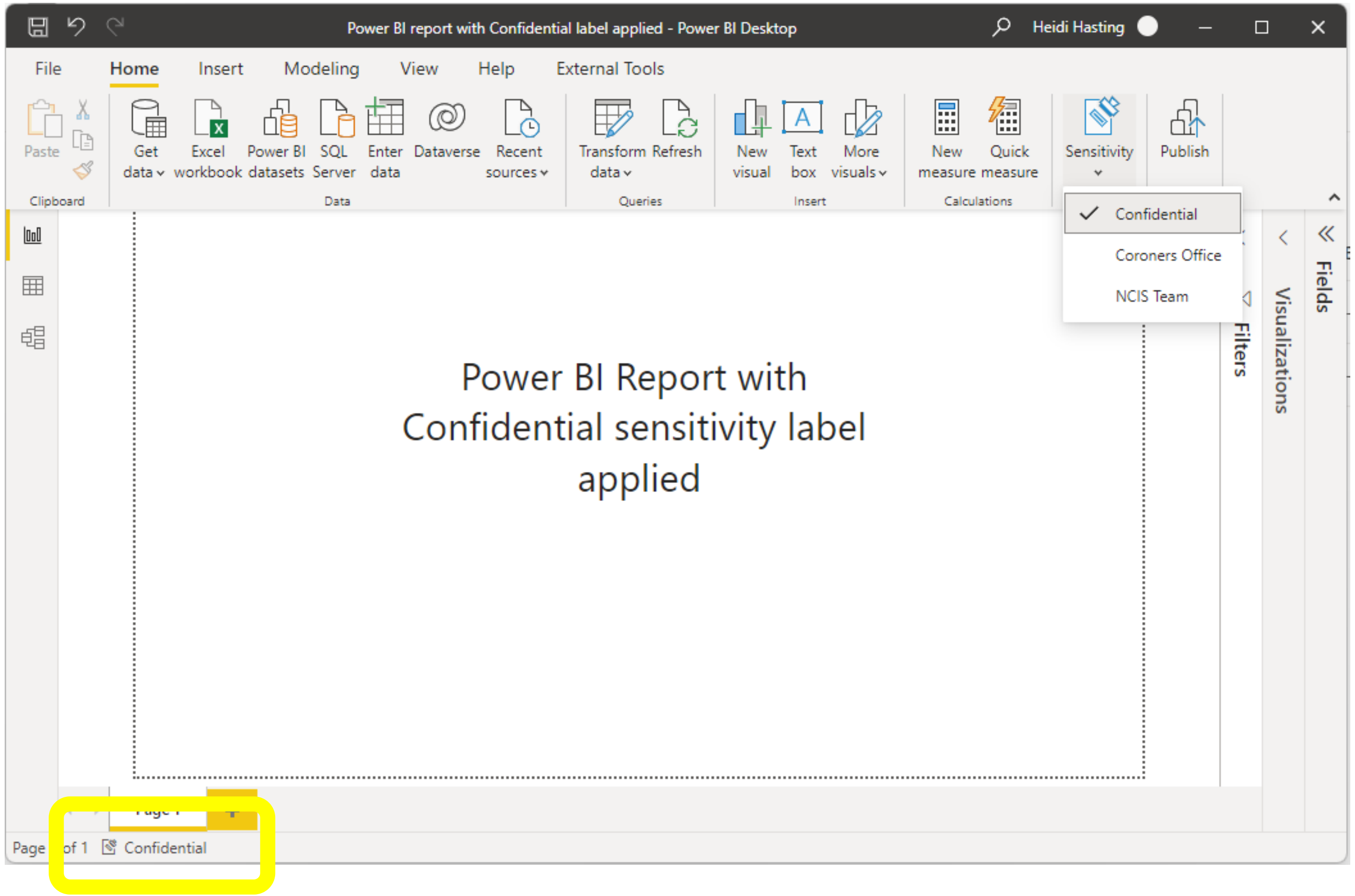


Sensitivity menu:

- ✓ Confidential
- Coroners Office
- NCIS Team

Power BI Report with Confidential sensitivity label applied

Power BI



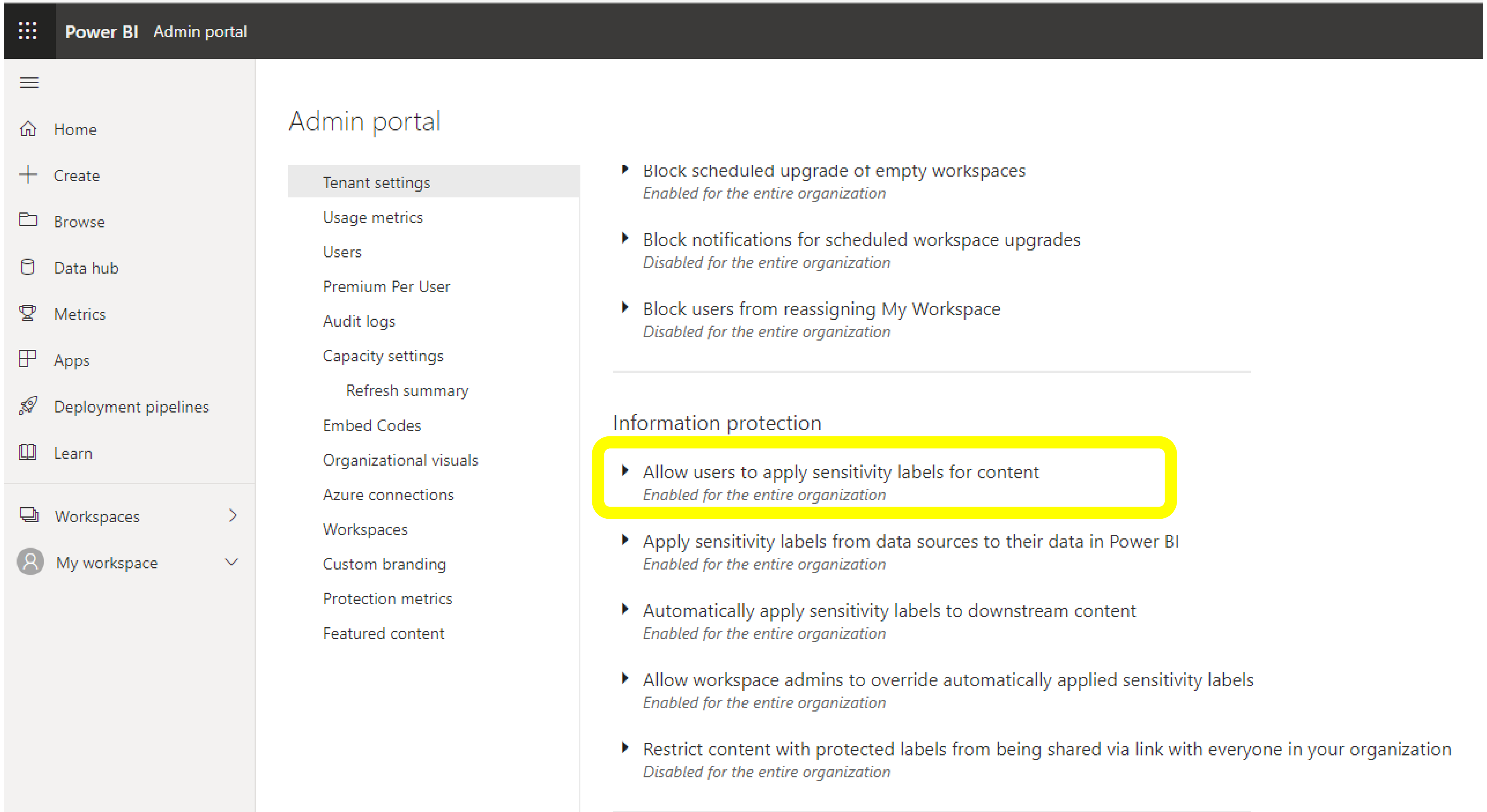
Power BI report with Confidential label applied - Power BI Desktop

Power BI Report with Confidential sensitivity label applied

Sensitivity: ✓ Confidential

Page 1 of 1 Confidential

Power BI Service – Setup



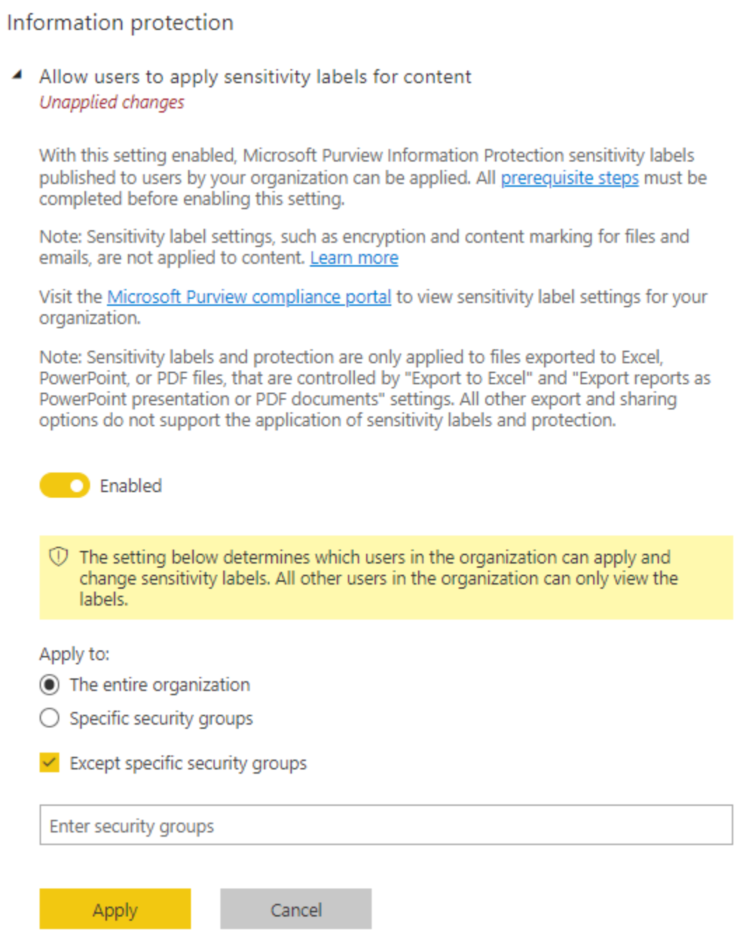
Admin portal

- Block scheduled upgrade of empty workspaces
  Enabled for the entire organization
- Block notifications for scheduled workspace upgrades
  Disabled for the entire organization
- Block users from reassigning My Workspace
  Disabled for the entire organization

Information protection

- Allow users to apply sensitivity labels for content
  Enabled for the entire organization
- Apply sensitivity labels from data sources to their data in Power BI
  Enabled for the entire organization
- Automatically apply sensitivity labels to downstream content
  Enabled for the entire organization
- Allow workspace admins to override automatically applied sensitivity labels
  Enabled for the entire organization
- Restrict content with protected labels from being shared via link with everyone in your organization
  Disabled for the entire organization

Information Protection



Information protection

Allow users to apply sensitivity labels for content
Unapplied changes

With this setting enabled, Microsoft Purview Information Protection sensitivity labels published to users by your organization can be applied. All prerequisite steps must be completed before enabling this setting.

Note: Sensitivity label settings, such as encryption and content marking for files and emails, are not applied to content. Learn more

Visit the Microsoft Purview compliance portal to view sensitivity label settings for your organization.

Note: Sensitivity labels and protection are only applied to files exported to Excel, PowerPoint, or PDF files, that are controlled by "Export to Excel" and "Export reports as PowerPoint presentation or PDF documents" settings. All other export and sharing options do not support the application of sensitivity labels and protection.

Enabled

The setting below determines which users in the organization can apply and change sensitivity labels. All other users in the organization can only view the labels.

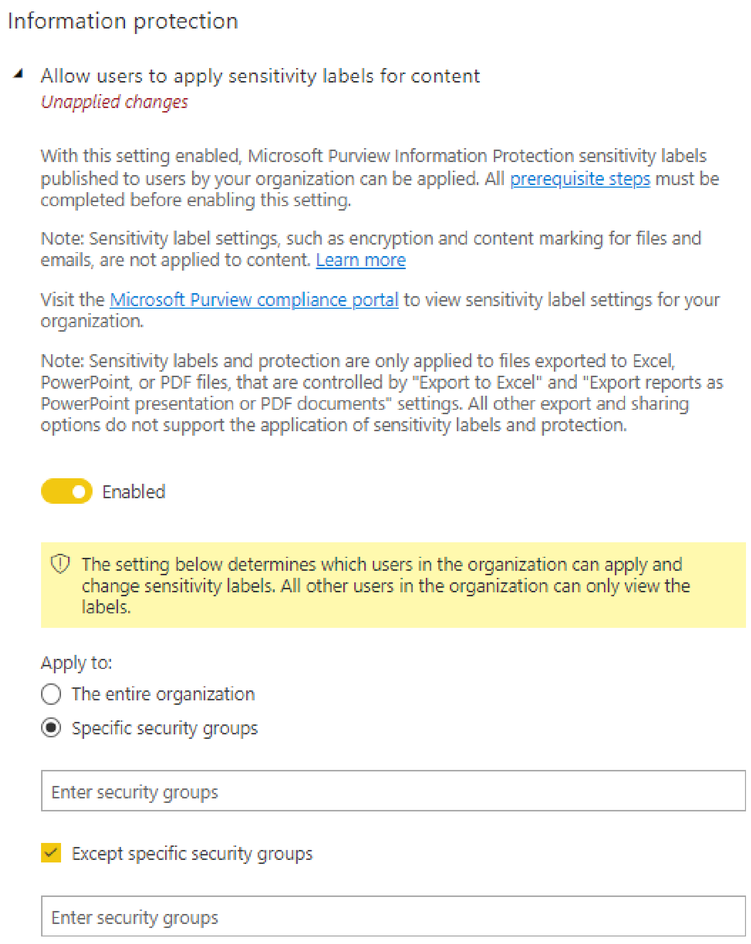
Apply to:

● The entire organization

○ Specific security groups

☑ Except specific security groups

Enter security groups



Information protection

Allow users to apply sensitivity labels for content
Unapplied changes

With this setting enabled, Microsoft Purview Information Protection sensitivity labels published to users by your organization can be applied. All prerequisite steps must be completed before enabling this setting.

Note: Sensitivity label settings, such as encryption and content marking for files and emails, are not applied to content. Learn more

Visit the Microsoft Purview compliance portal to view sensitivity label settings for your organization.

Note: Sensitivity labels and protection are only applied to files exported to Excel, PowerPoint, or PDF files, that are controlled by "Export to Excel" and "Export reports as PowerPoint presentation or PDF documents" settings. All other export and sharing options do not support the application of sensitivity labels and protection.

Enabled

The setting below determines which users in the organization can apply and change sensitivity labels. All other users in the organization can only view the labels.

Apply to:

○ The entire organization

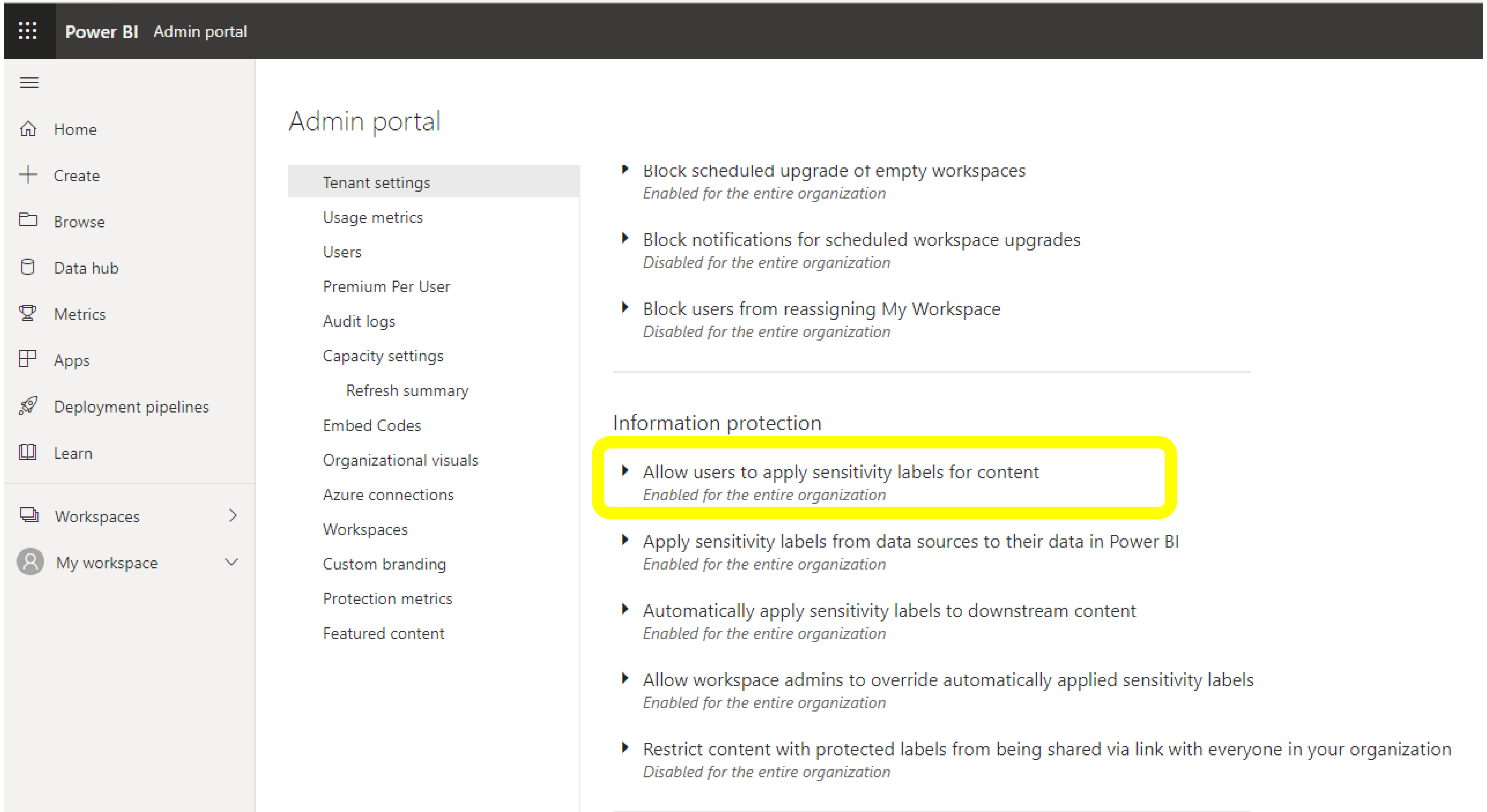
● Specific security groups

Enter security groups

☑ Except specific security groups

Enter security groups

Power BI Service – Setup



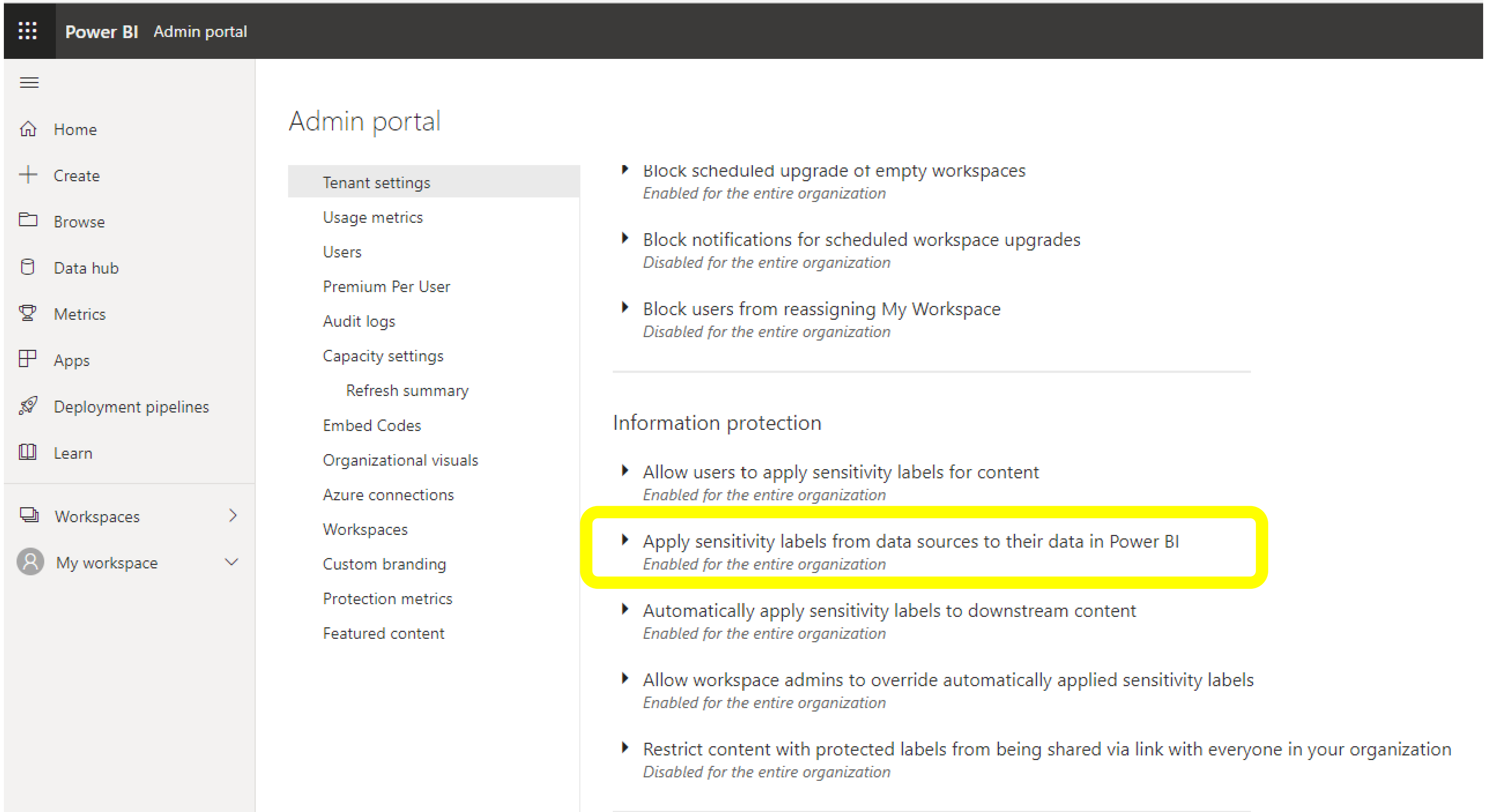
Admin portal

- Block scheduled upgrade of empty workspaces
  Enabled for the entire organization
- Block notifications for scheduled workspace upgrades
  Disabled for the entire organization
- Block users from reassigning My Workspace
  Disabled for the entire organization

Information protection

- Allow users to apply sensitivity labels for content
  Enabled for the entire organization
- Apply sensitivity labels from data sources to their data in Power BI
  Enabled for the entire organization
- Automatically apply sensitivity labels to downstream content
  Enabled for the entire organization
- Allow workspace admins to override automatically applied sensitivity labels
  Enabled for the entire organization
- Restrict content with protected labels from being shared via link with everyone in your organization
  Disabled for the entire organization

Power BI Service – Setup



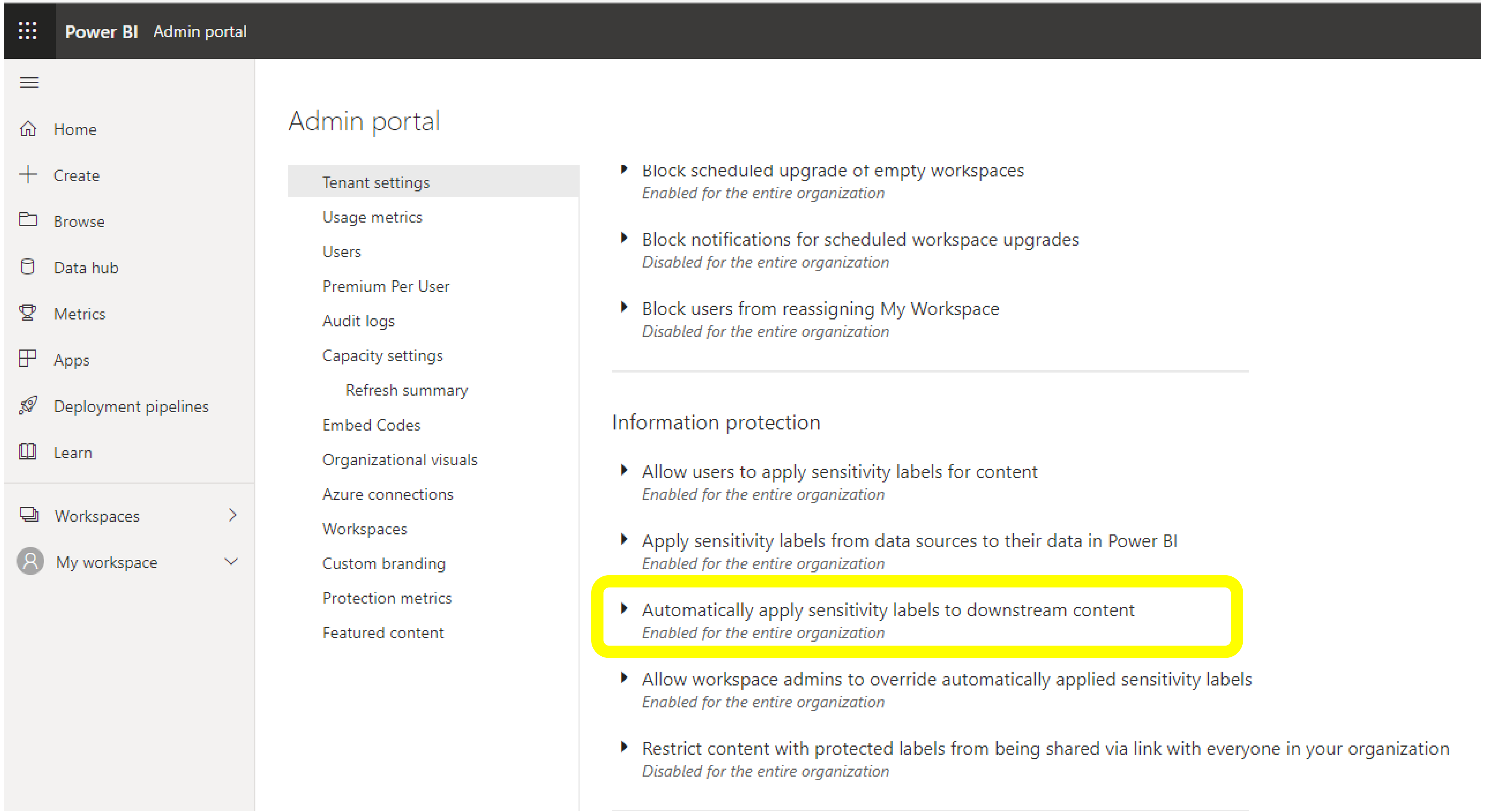
Admin portal

- Block scheduled upgrade of empty workspaces
  Enabled for the entire organization
- Block notifications for scheduled workspace upgrades
  Disabled for the entire organization
- Block users from reassigning My Workspace
  Disabled for the entire organization

Information protection

- Allow users to apply sensitivity labels for content
  Enabled for the entire organization
- Apply sensitivity labels from data sources to their data in Power BI
  Enabled for the entire organization
- Automatically apply sensitivity labels to downstream content
  Enabled for the entire organization
- Allow workspace admins to override automatically applied sensitivity labels
  Enabled for the entire organization
- Restrict content with protected labels from being shared via link with everyone in your organization
  Disabled for the entire organization

Power BI Service – Setup



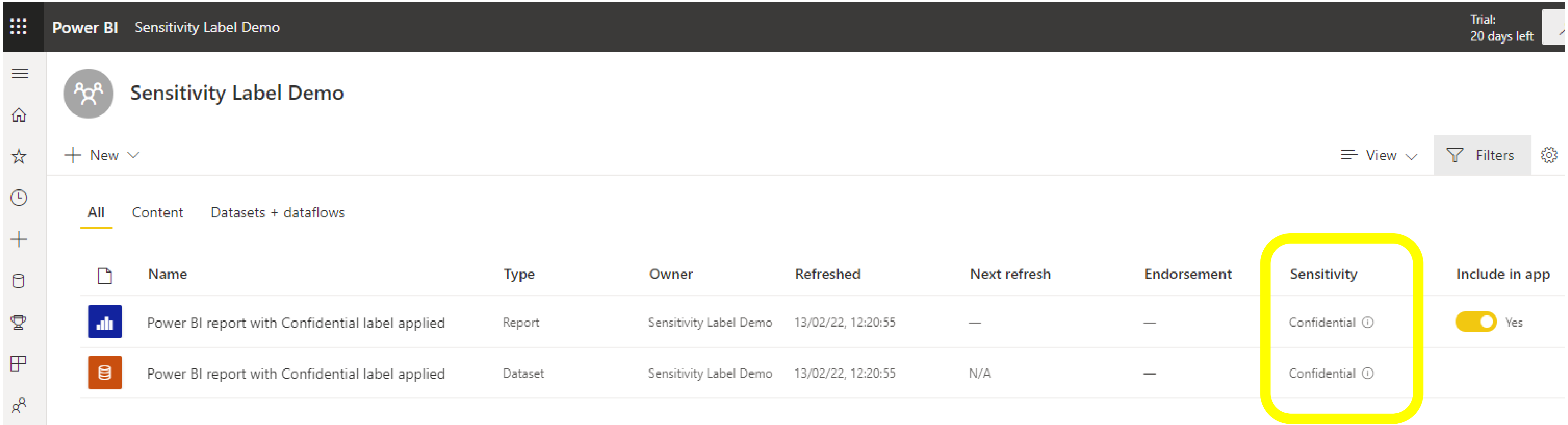
Admin portal

- Block scheduled upgrade of empty workspaces
  Enabled for the entire organization
- Block notifications for scheduled workspace upgrades
  Disabled for the entire organization
- Block users from reassigning My Workspace
  Disabled for the entire organization

Information protection

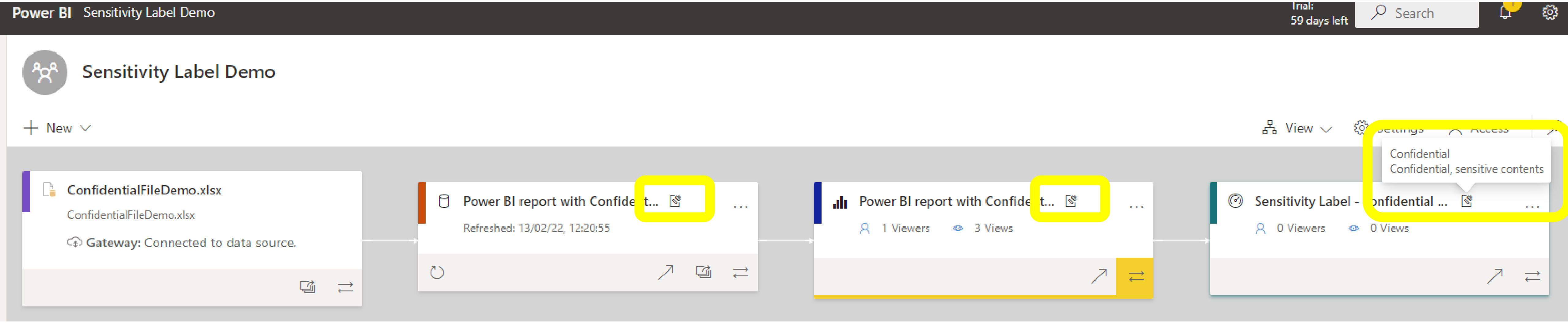
- Allow users to apply sensitivity labels for content
  Enabled for the entire organization
- Apply sensitivity labels from data sources to their data in Power BI
  Enabled for the entire organization
- Automatically apply sensitivity labels to downstream content
  Enabled for the entire organization
- Allow workspace admins to override automatically applied sensitivity labels
  Enabled for the entire organization
- Restrict content with protected labels from being shared via link with everyone in your organization
  Disabled for the entire organization

Power BI Service – list view

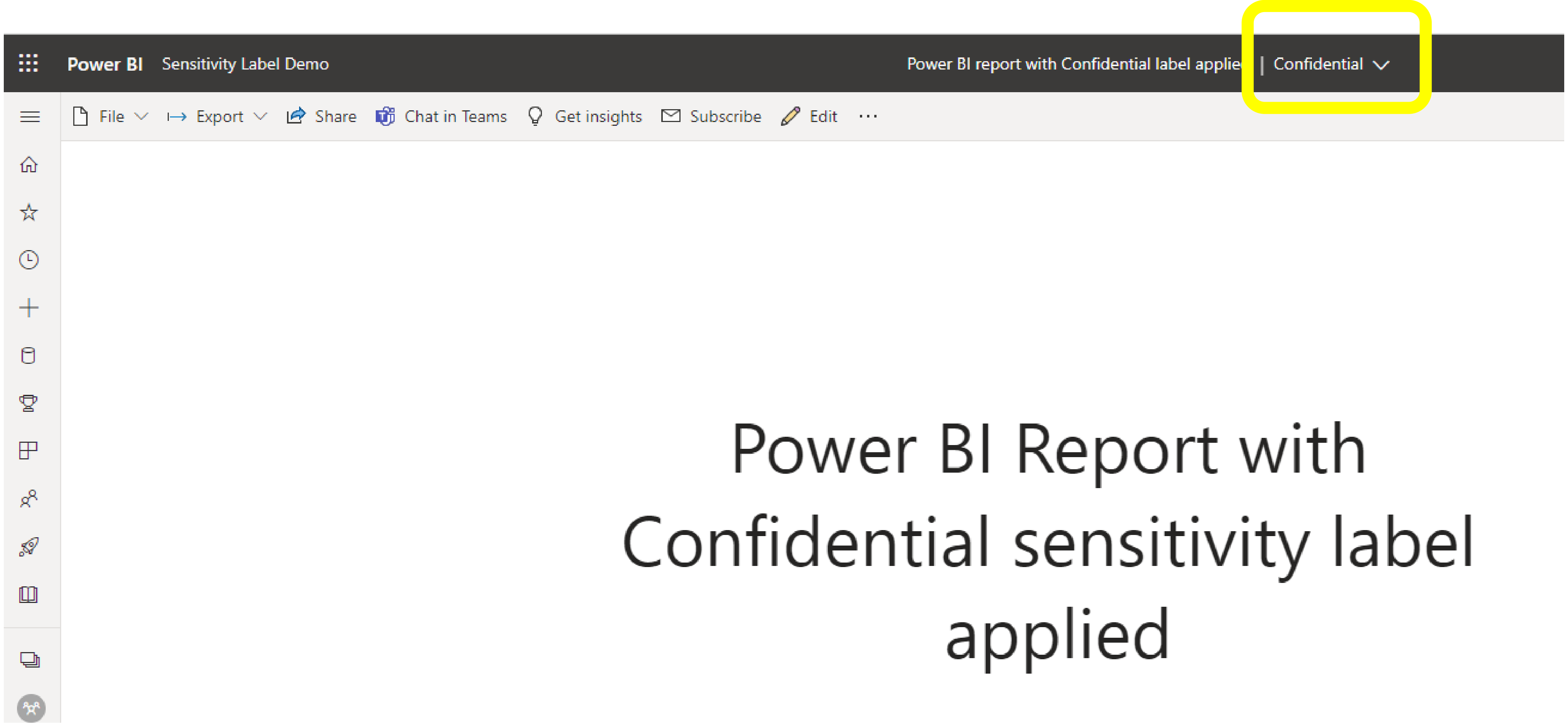


Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Include in app
Power BI report with Confidential label applied	Report	Sensitivity Label Demo	13/02/22, 12:20:55	—	—	Confidential ⓘ	Yes
Power BI report with Confidential label applied	Dataset	Sensitivity Label Demo	13/02/22, 12:20:55	N/A	—	Confidential ⓘ	

Power BI Service – lineage view

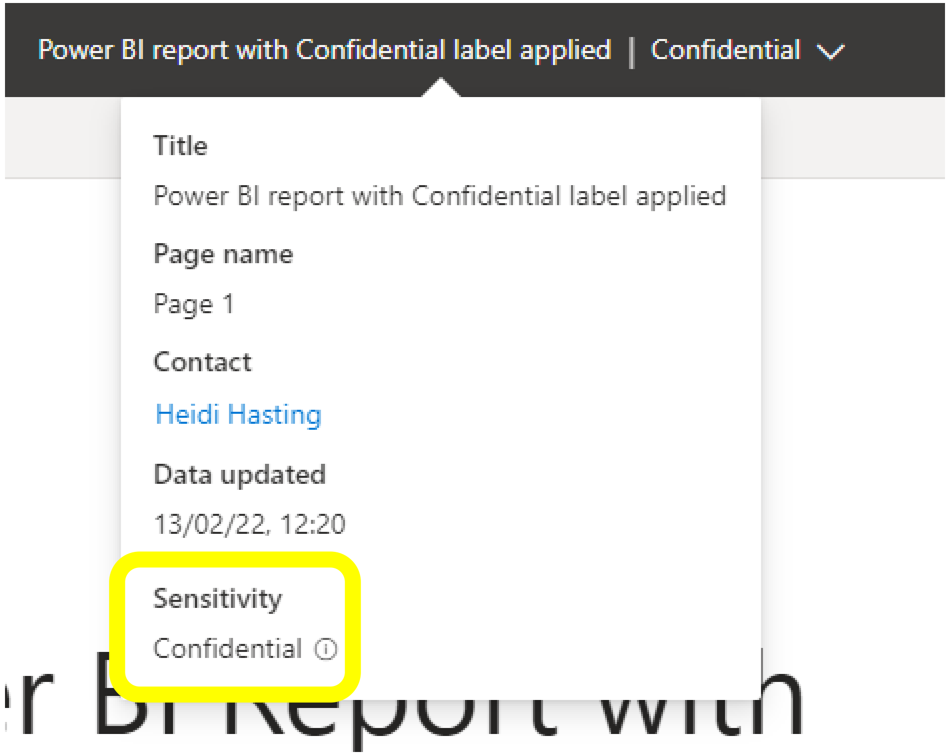

Power BI
Sensitivity Label Demo
Trial:
59 days left
Search
Sensitivity Label Demo
New
View
Settings
Access
Confidential
Confidential, sensitive contents
ConfidentialFileDemo.xlsx
ConfidentialFileDemo.xlsx
Gateway: Connected to data source.
Power BI report with Confide t...
Refreshed: 13/02/22, 12:20:55
Power BI report with Confide t...
1 Viewers
3 Views
Sensitivity Label - onfidential ...
0 Viewers
0 Views

Power BI Service - report



Power BI Report with Confidential sensitivity label applied

Power BI Service - report



Power BI report with Confidential label applied | Confidential

Title

Power BI report with Confidential label applied

Page name

Page 1

Contact

Heidi Hasting

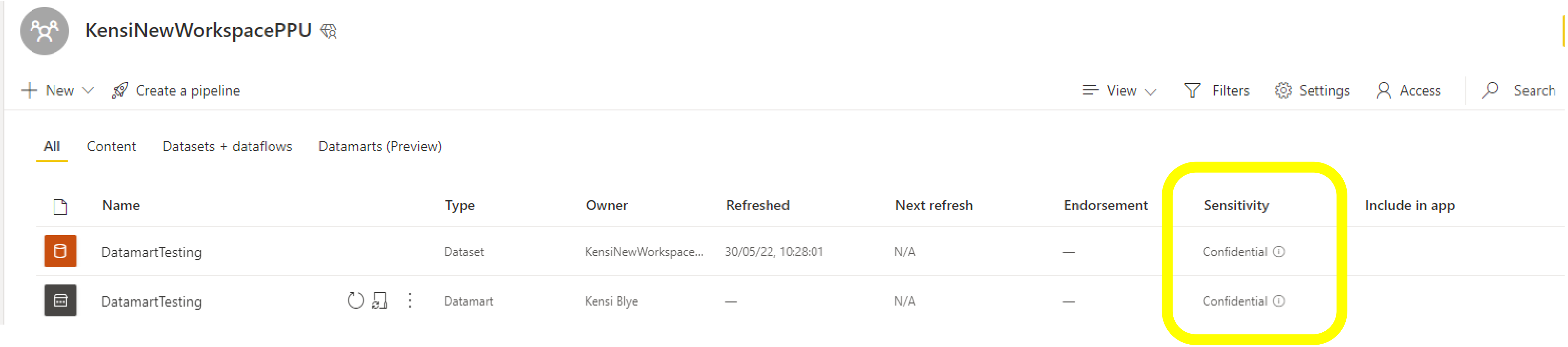
Data updated

13/02/22, 12:20

Sensitivity

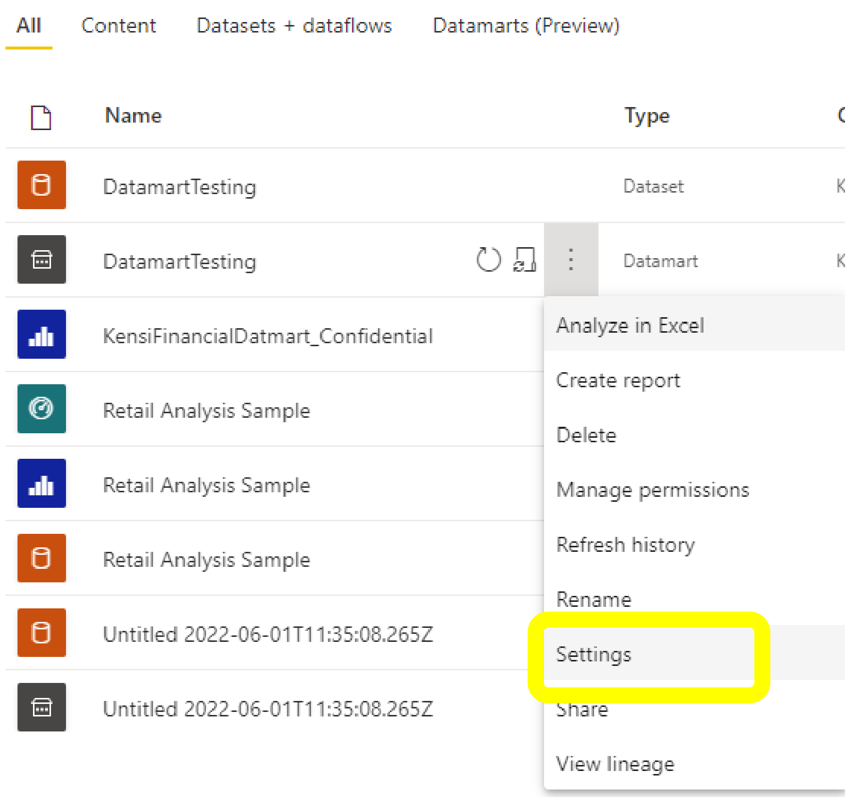
Confidential ⓘ

Datamart

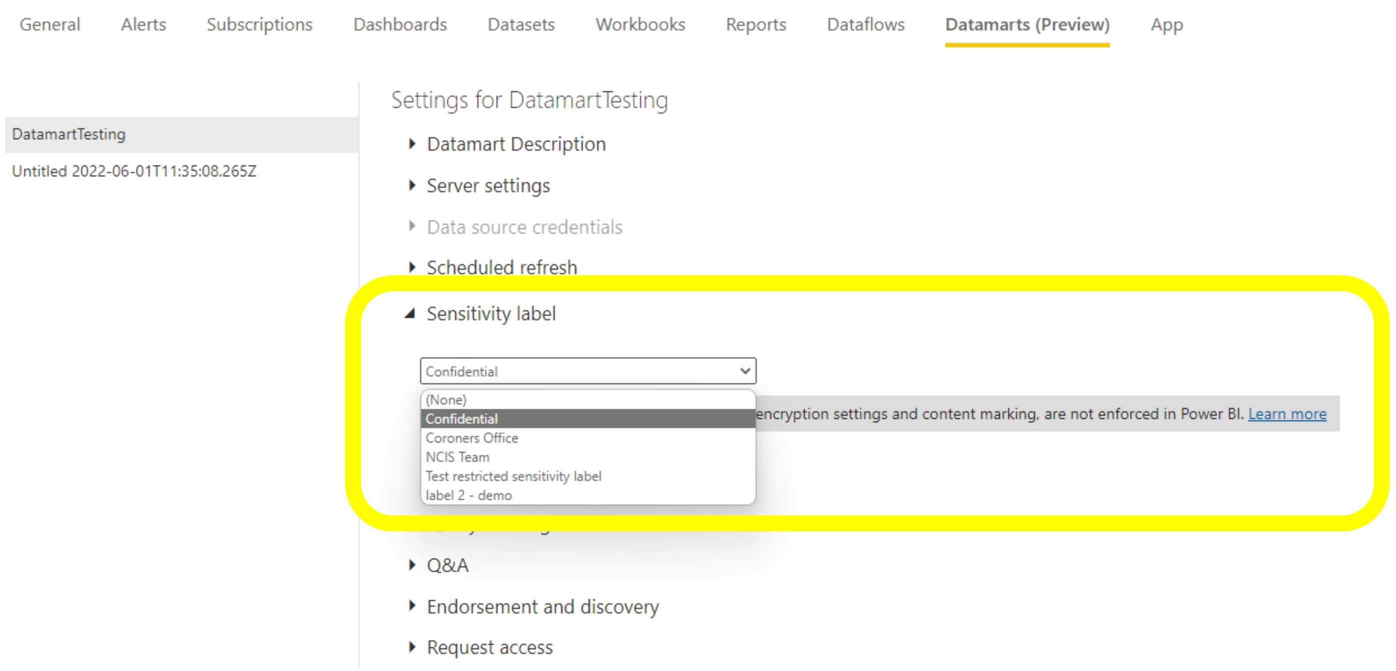


Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Include in app
DatamartTesting	Dataset	KensiNewWorkspace...	30/05/22, 10:28:01	N/A	—	Confidential ⓘ	
DatamartTesting	Datamart	Kensi Blye	—	N/A	—	Confidential ⓘ	

Datamart



Name	Type
DatamartTesting	Dataset
DatamartTesting	Datamart
KensiFinancialDatmart_Confidential	
Retail Analysis Sample	
Retail Analysis Sample	
Retail Analysis Sample	
Untitled 2022-06-01T11:35:08.265Z	
Untitled 2022-06-01T11:35:08.265Z	

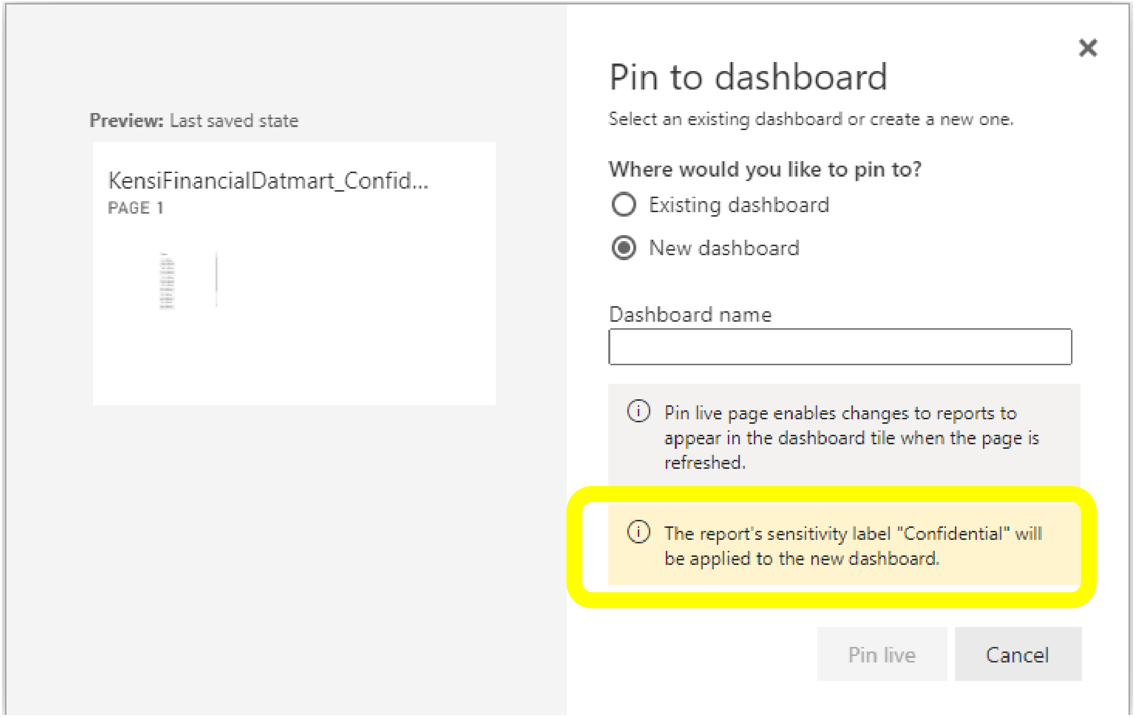


Settings for DatamartTesting

Sensitivity label: Confidential

encryption settings and content marking, are not enforced in Power BI. Learn more

Dashboard - new



Preview: Last saved state

KensiFinancialDatmart_Confid...
PAGE 1

Pin to dashboard

Select an existing dashboard or create a new one.

Where would you like to pin to?

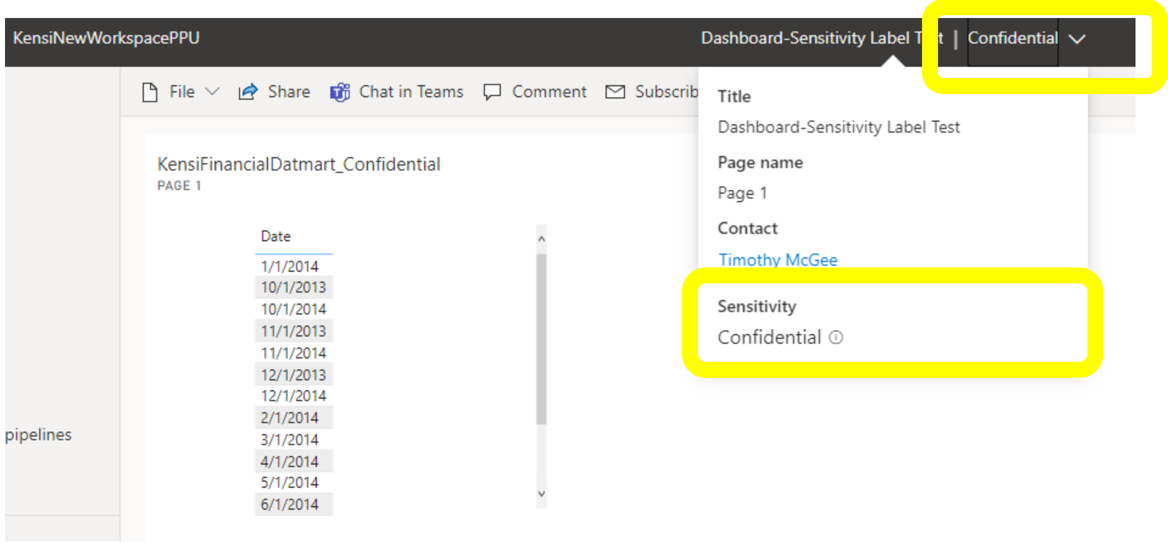
○ Existing dashboard

● New dashboard

Dashboard name

ⓘ Pin live page enables changes to reports to appear in the dashboard tile when the page is refreshed.

ⓘ The report's sensitivity label "Confidential" will be applied to the new dashboard.



KensiNewWorkspacePPU

Dashboard-Sensitivity Label T t | Confidential

KensiFinancialDatmart_Confidential
PAGE 1

Date
1/1/2014
10/1/2013
10/1/2014
11/1/2013
11/1/2014
12/1/2013
12/1/2014
2/1/2014
3/1/2014
4/1/2014
5/1/2014
6/1/2014

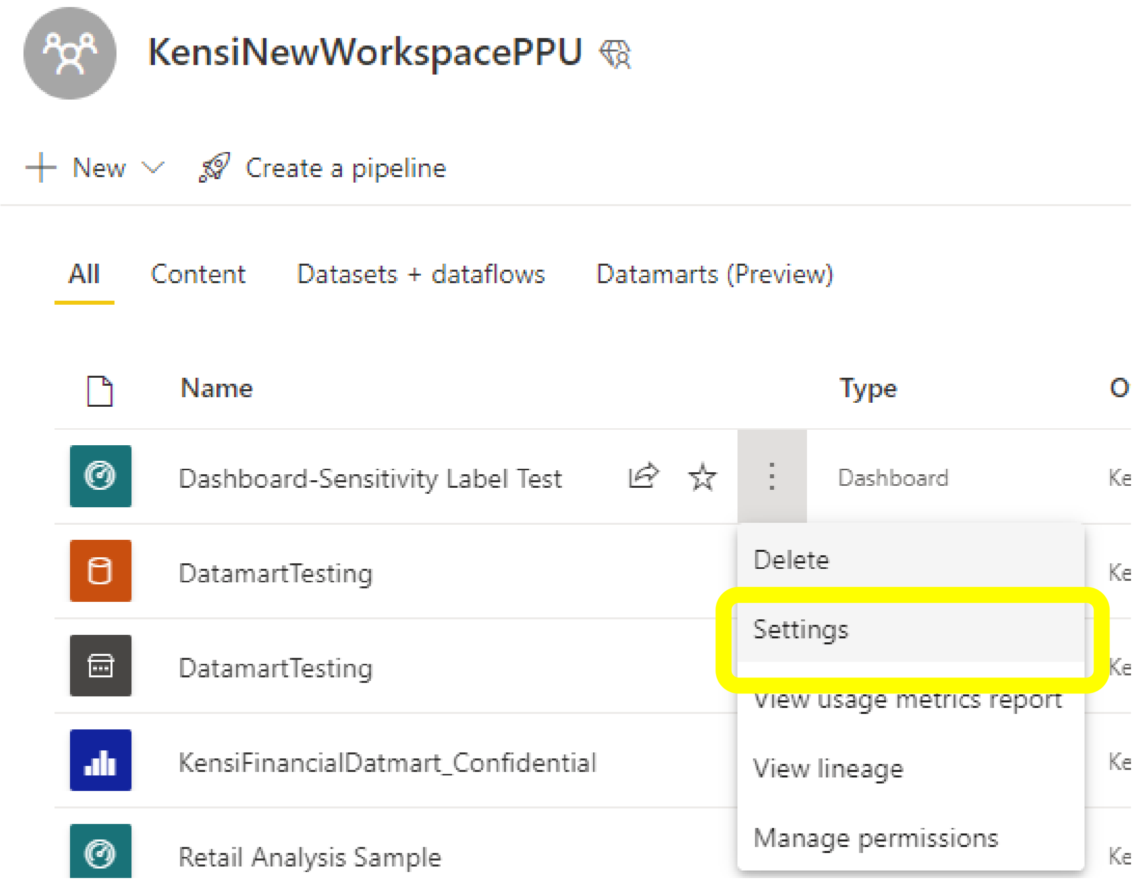
Title
Dashboard-Sensitivity Label Test

Page name
Page 1

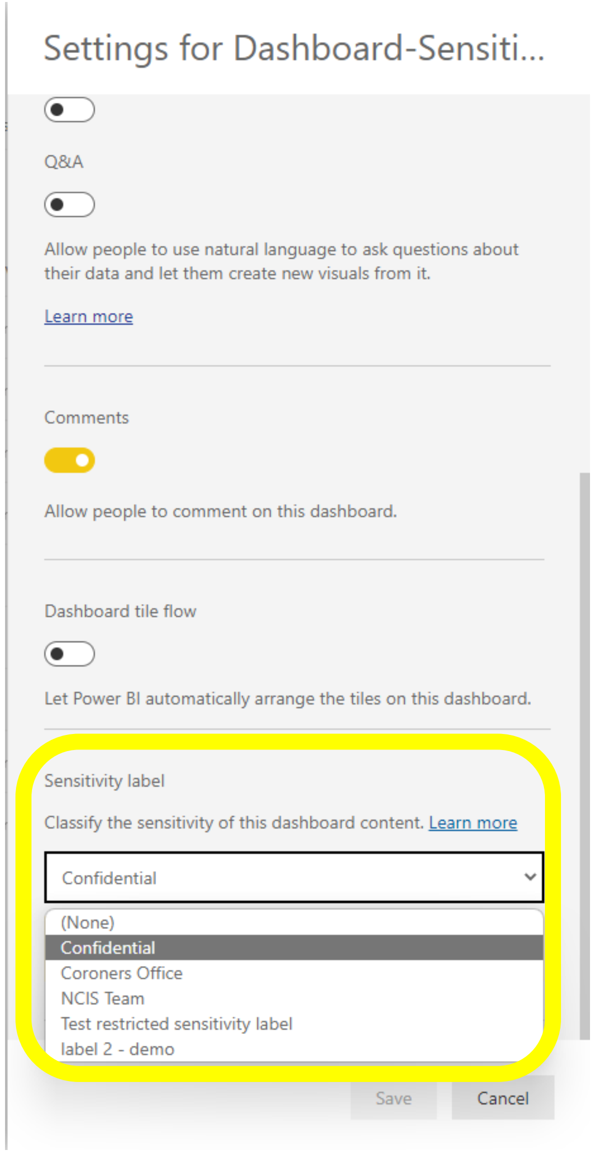
Contact
Timothy McGee

Sensitivity
Confidential ⓘ

Dashboard - continued



Name	Type	O
Dashboard-Sensitivity Label Test	Dashboard	Ke
DatamartTesting		Ke
DatamartTesting		Ke
KensiFinancialDatmart_Confidential		Ke
Retail Analysis Sample		Ke



Settings for Dashboard-Sensiti...

Q&A

Allow people to use natural language to ask questions about their data and let them create new visuals from it.

Learn more

Comments

Allow people to comment on this dashboard.

Dashboard tile flow

Let Power BI automatically arrange the tiles on this dashboard.

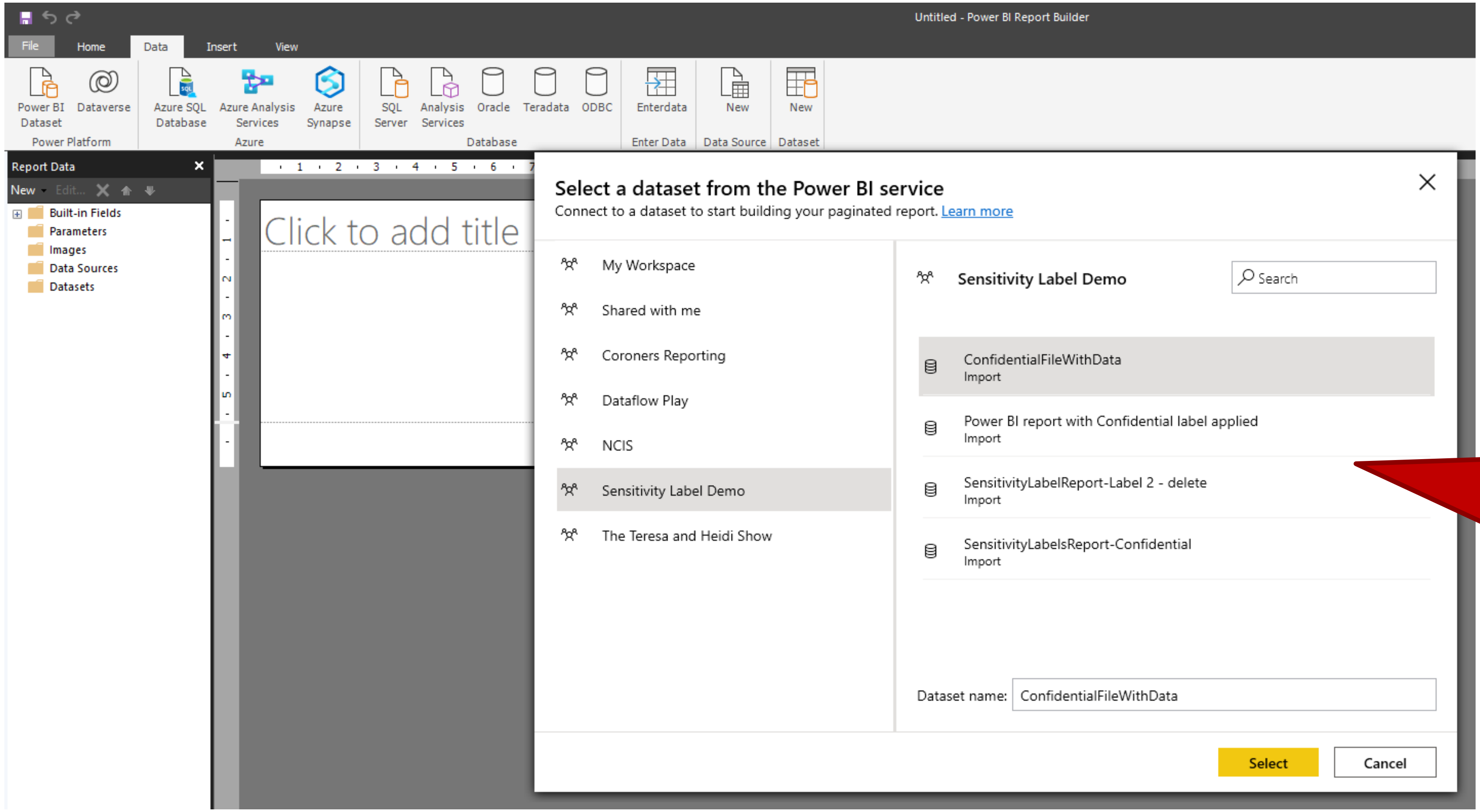
Sensitivity label

Classify the sensitivity of this dashboard content. Learn more

Confidential

(None)
Confidential
Coroners Office
NCIS Team
Test restricted sensitivity label
label 2 - demo

Paginated Report – Power BI Report Builder



Select a dataset from the Power BI service

Connect to a dataset to start building your paginated report. Learn more

- My Workspace
- Shared with me
- Coroners Reporting
- Dataflow Play
- NCIS
- Sensitivity Label Demo
- The Teresa and Heidi Show

Sensitivity Label Demo

Search

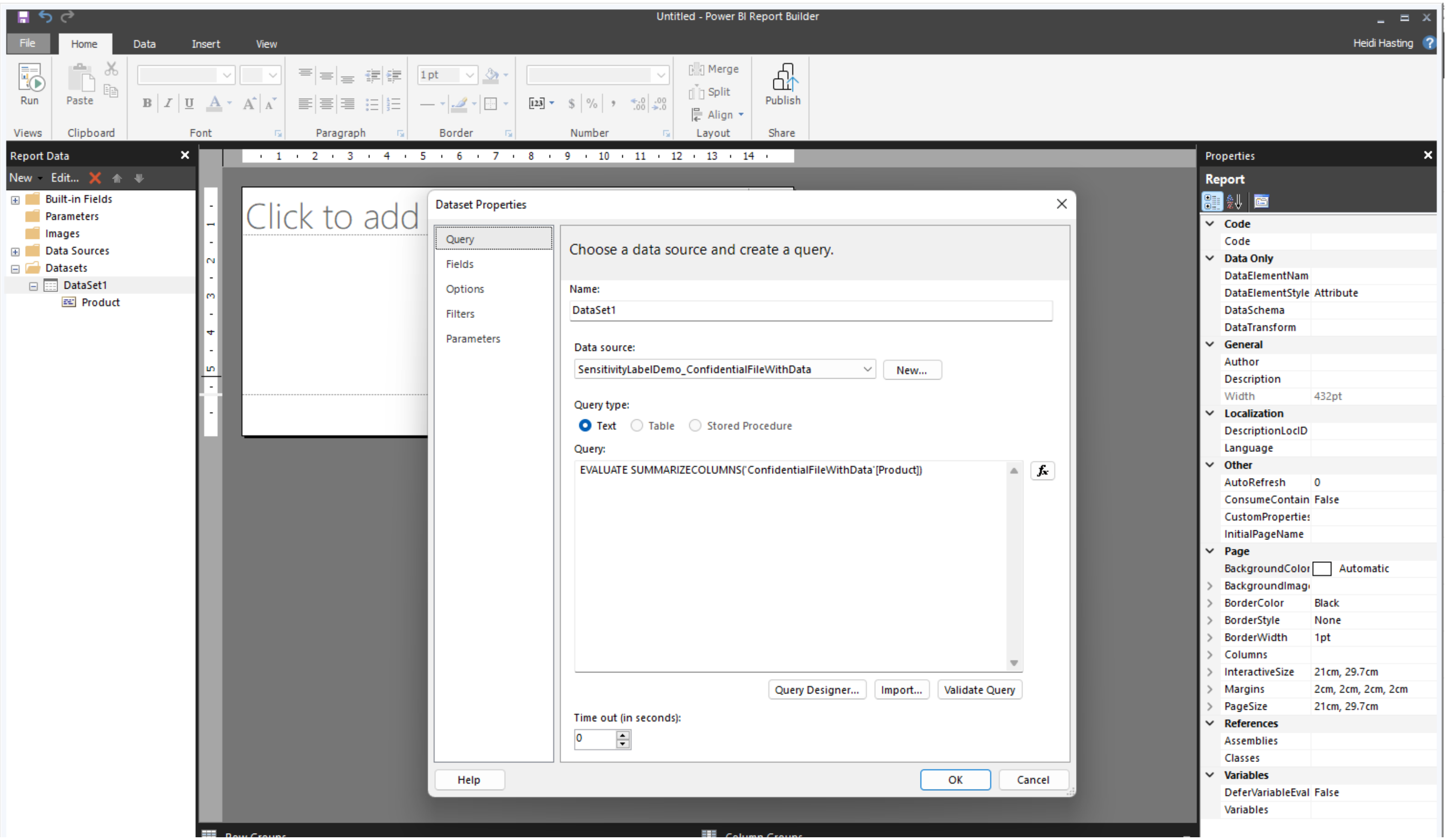
- ConfidentialFileWithData
  Import
- Power BI report with Confidential label applied
  Import
- SensitivityLabelReport-Label 2 - delete
  Import
- SensitivityLabelsReport-Confidential
  Import

Dataset name: ConfidentialFileWithData

Select Cancel

Power BI Dataset
No sensitivity label information is shown

Power BI Report Builder



Dataset Properties

Query | Fields | Options | Filters | Parameters

Choose a data source and create a query.

Name: DataSet1

Data source: SensitivityLabelDemo_ConfidentialFileWithData

Query type: ● Text ○ Table ○ Stored Procedure

Query:

```
EVALUATE SUMMARIZECOLUMNS('ConfidentialFileWithData'[Product])
```

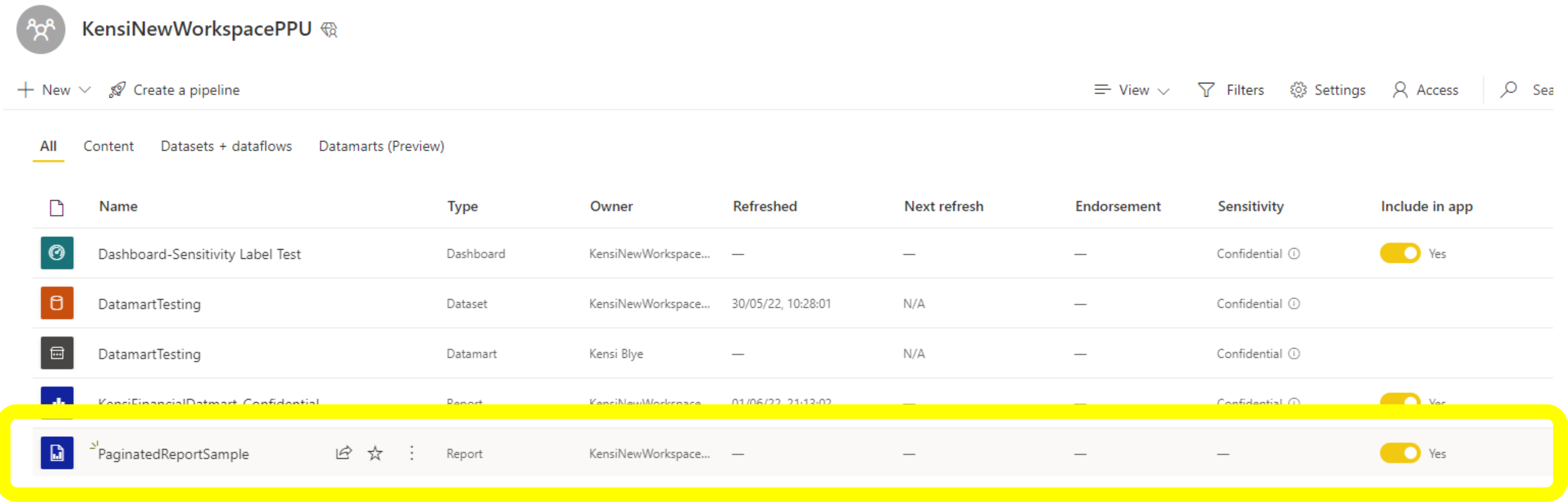
Time out (in seconds): 0

Properties

Report

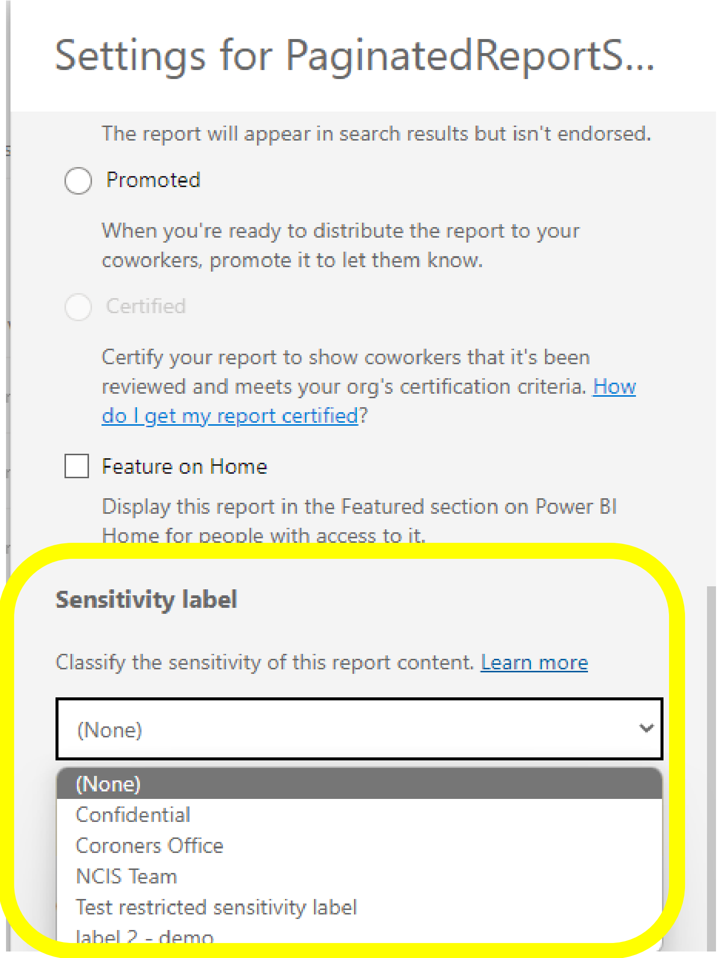
Code	
Code	
Data Only	
DataElementNam	
DataElementStyle	Attribute
DataSchema	
DataTransform	
General	
Author	
Description	
Width	432pt
Localization	
DescriptionLocID	
Language	
Other	
AutoRefresh	0
ConsumeContain	False
CustomPropertie:	
InitialPageName	
Page	
BackgroundColor	□ Automatic
BackgroundImag	
BorderColor	Black
BorderStyle	None
BorderWidth	1pt
Columns	
InteractiveSize	21cm, 29.7cm
Margins	2cm, 2cm, 2cm, 2cm
PageSize	21cm, 29.7cm
References	
Assemblies	
Classes	
Variables	
DeferVariableEval	False
Variables	

Paginated Report – apply in Power BI Service



KensiNewWorkspacePPU

Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Include in app
Dashboard-Sensitivity Label Test	Dashboard	KensiNewWorkspace...	—	—	—	Confidential ⓘ	Yes
DatamartTesting	Dataset	KensiNewWorkspace...	30/05/22, 10:28:01	N/A	—	Confidential ⓘ	
DatamartTesting	Datamart	Kensi Blye	—	N/A	—	Confidential ⓘ	
KensiFinancialDatamart_Confidential	Report	KensiNewWorkspace...	01/06/22, 21:13:02	—	—	Confidential ⓘ	Yes
PaginatedReportSample	Report	KensiNewWorkspace...	—	—	—	—	Yes



Settings for PaginatedReportS...

The report will appear in search results but isn't endorsed.

○ Promoted

When you're ready to distribute the report to your coworkers, promote it to let them know.

○ Certified

Certify your report to show coworkers that it's been reviewed and meets your org's certification criteria. How do I get my report certified?

□ Feature on Home

Display this report in the Featured section on Power BI Home for people with access to it.

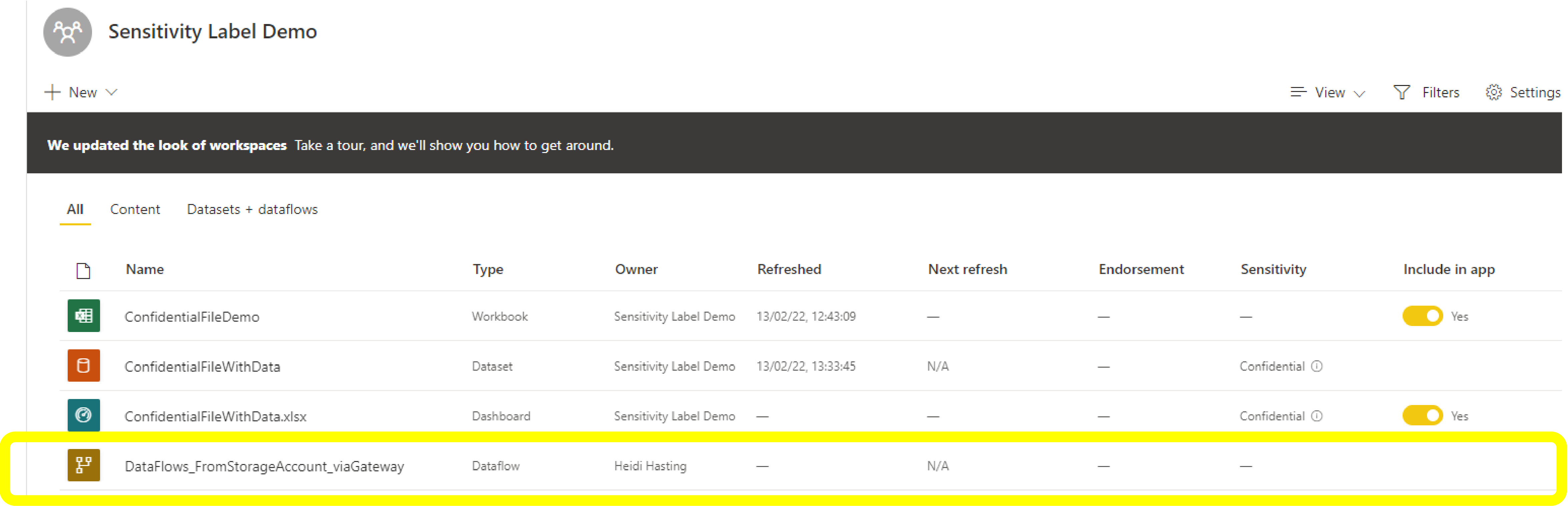
Sensitivity label

Classify the sensitivity of this report content. Learn more

(None)

- (None)
- Confidential
- Coroners Office
- NCIS Team
- Test restricted sensitivity label
- label 2 - demo

Data Flows

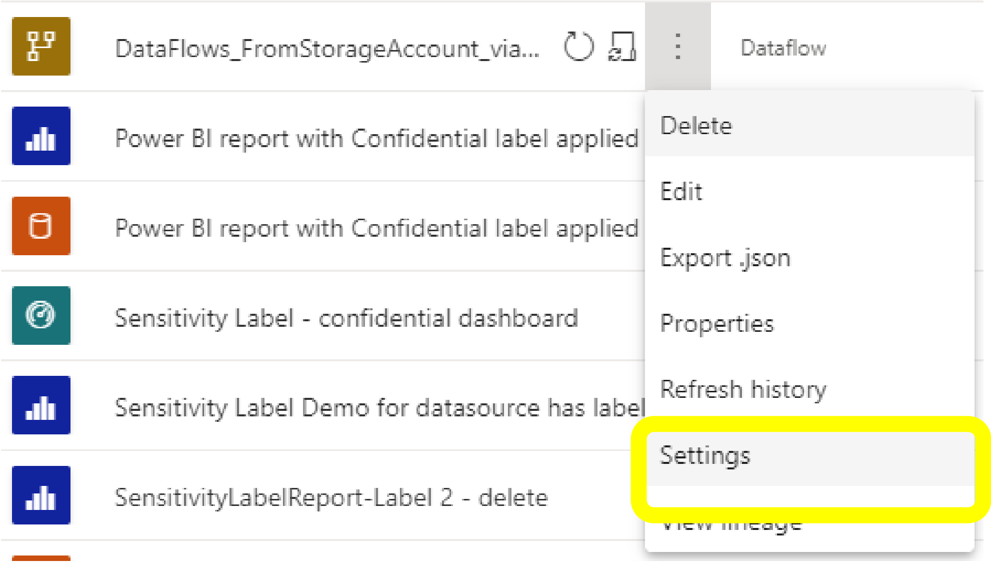


Sensitivity Label Demo

We updated the look of workspaces Take a tour, and we'll show you how to get around.

	Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Include in app
	ConfidentialFileDemo	Workbook	Sensitivity Label Demo	13/02/22, 12:43:09	—	—	—	Yes
	ConfidentialFileWithData	Dataset	Sensitivity Label Demo	13/02/22, 13:33:45	N/A	—	Confidential ⓘ	
	ConfidentialFileWithData.xlsx	Dashboard	Sensitivity Label Demo	—	—	—	Confidential ⓘ	Yes
	DataFlows_FromStorageAccount_viaGateway	Dataflow	Heidi Hasting	—	N/A	—	—	

Data Flows



DataFlows_FromStorageAccount_via... Dataflow

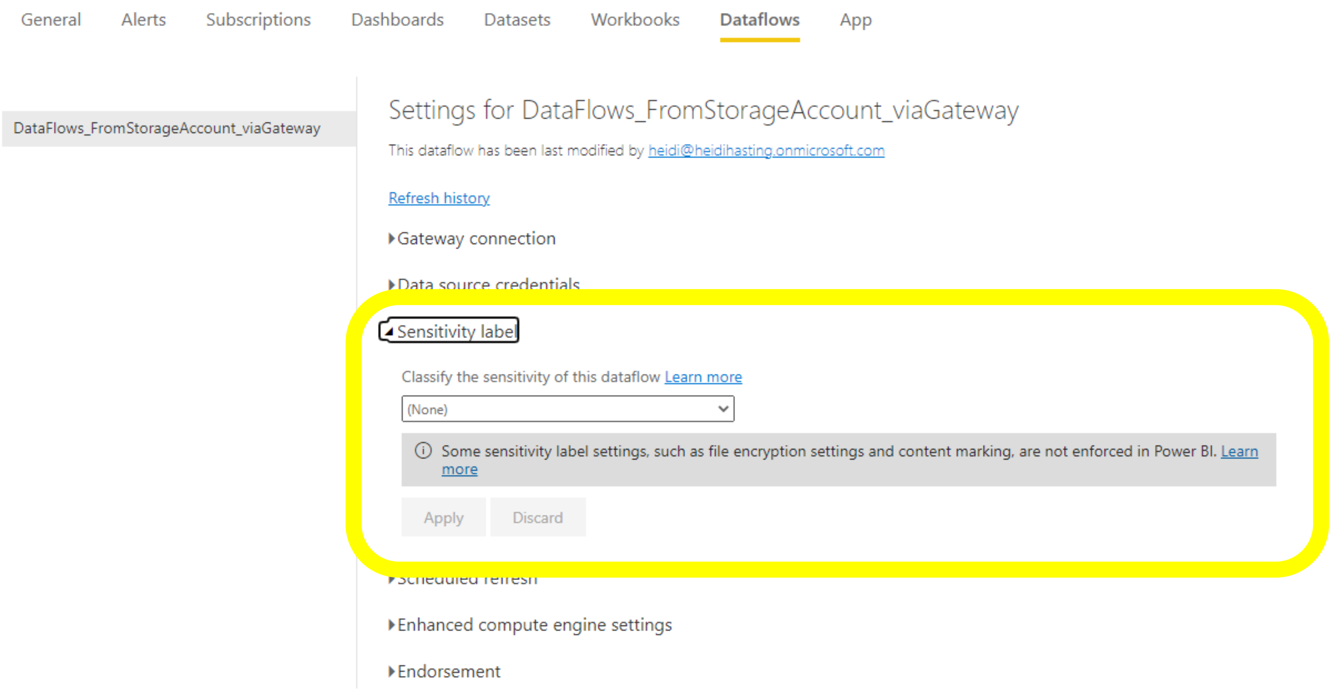
Power BI report with Confidential label applied

Power BI report with Confidential label applied

Sensitivity Label - confidential dashboard

Sensitivity Label Demo for datasource has label

SensitivityLabelReport-Label 2 - delete



Settings for DataFlows_FromStorageAccount_viaGateway

This dataflow has been last modified by heidi@heidihasting.onmicrosoft.com

Refresh history

▸Gateway connection

▸Data source credentials

◂Sensitivity label

Classify the sensitivity of this dataflow Learn more

(None)

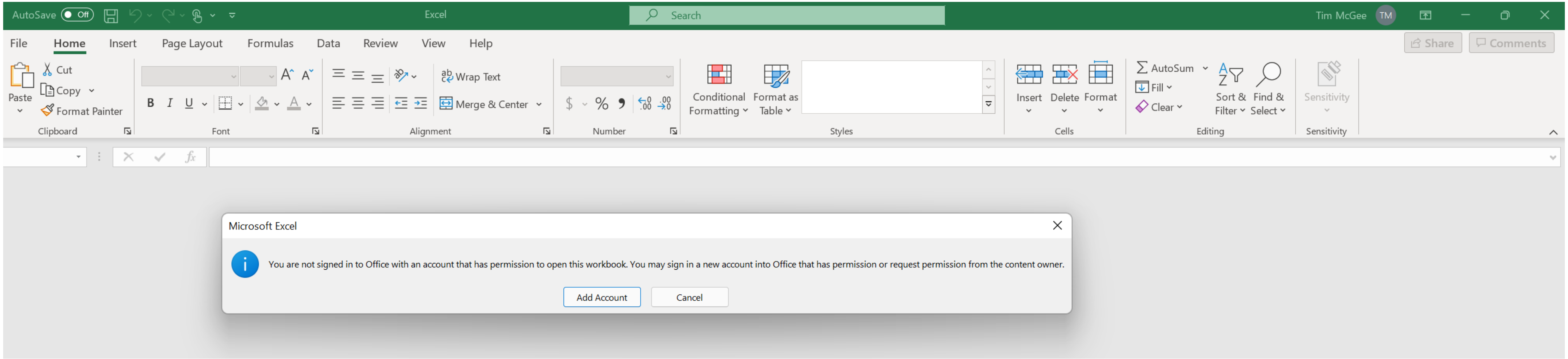
ⓘ Some sensitivity label settings, such as file encryption settings and content marking, are not enforced in Power BI. Learn more

▸Scheduled refresh

▸Enhanced compute engine settings

▸Endorsement

Power BI – Export to Excel error

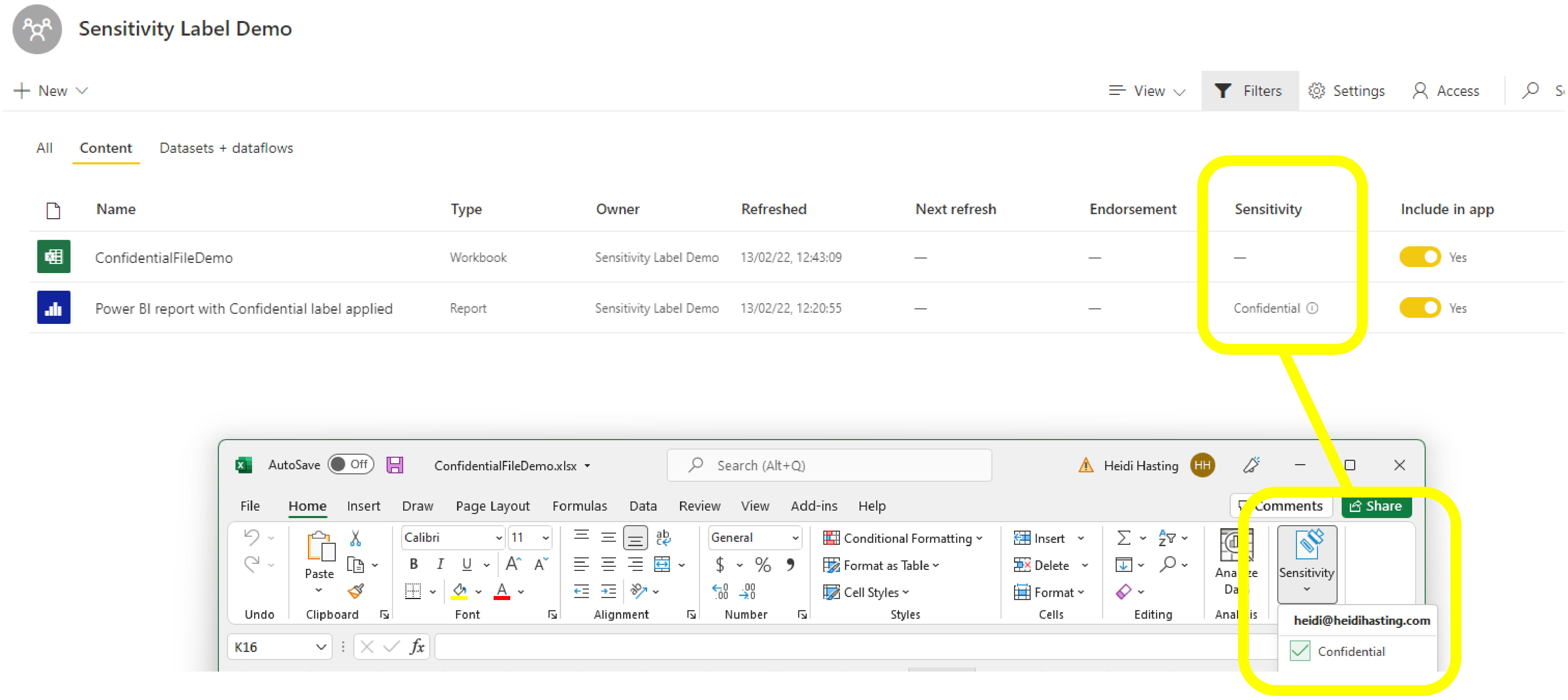


Microsoft Excel

You are not signed in to Office with an account that has permission to open this workbook. You may sign in a new account into Office that has permission or request permission from the content owner.

Add Account | Cancel

Excel file with sensitivity label applied doesn't show sensitivity label in Power BI



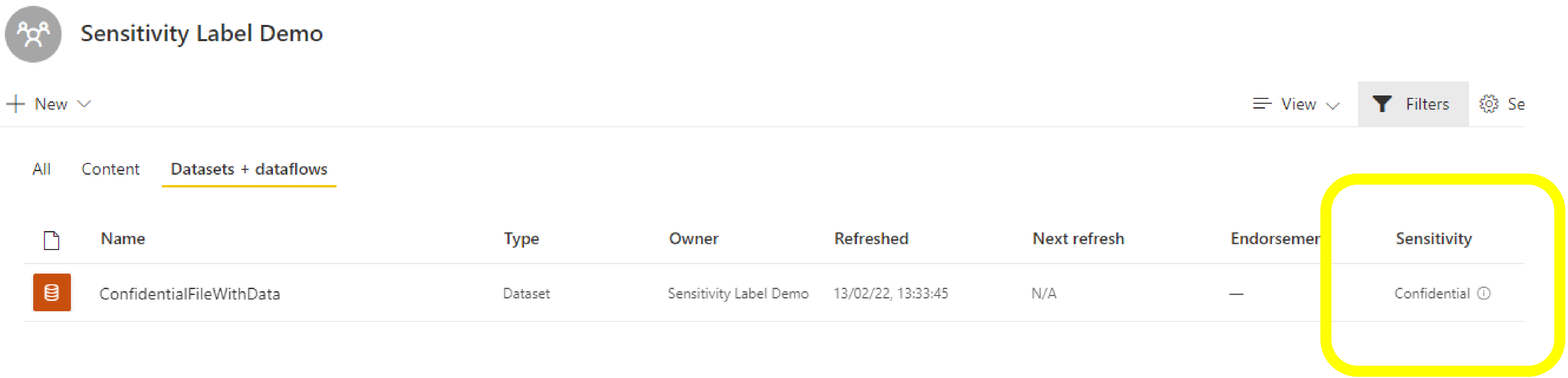
Sensitivity Label Demo

	Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Include in app
	ConfidentialFileDemo	Workbook	Sensitivity Label Demo	13/02/22, 12:43:09	—	—	—	Yes
	Power BI report with Confidential label applied	Report	Sensitivity Label Demo	13/02/22, 12:20:55	—	—	Confidential ⓘ	Yes

heidi@heidihasting.com

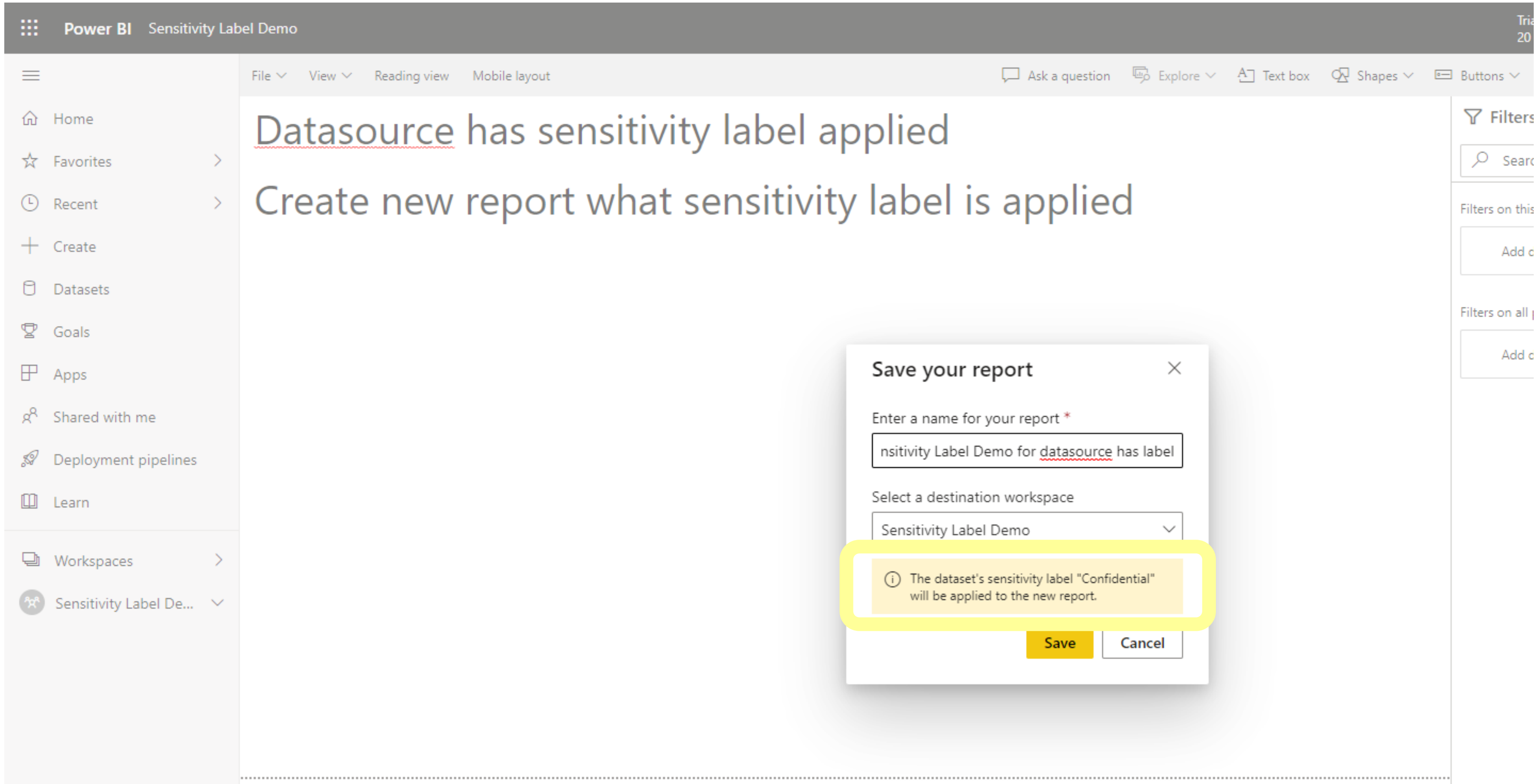
☑ Confidential

Create report using dataset that has sensitivity label already applied



	Name	Type	Owner	Refreshed	Next refresh	Endorsemer	Sensitivity
	ConfidentialFileWithData	Dataset	Sensitivity Label Demo	13/02/22, 13:33:45	N/A	—	Confidential ⓘ

Create report using dataset that has sensitivity label already applied



Datasource has sensitivity label applied

Create new report what sensitivity label is applied

Save your report

Enter a name for your report *

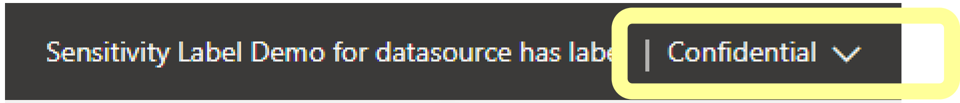
nsitivity Label Demo for datasource has label

Select a destination workspace

Sensitivity Label Demo

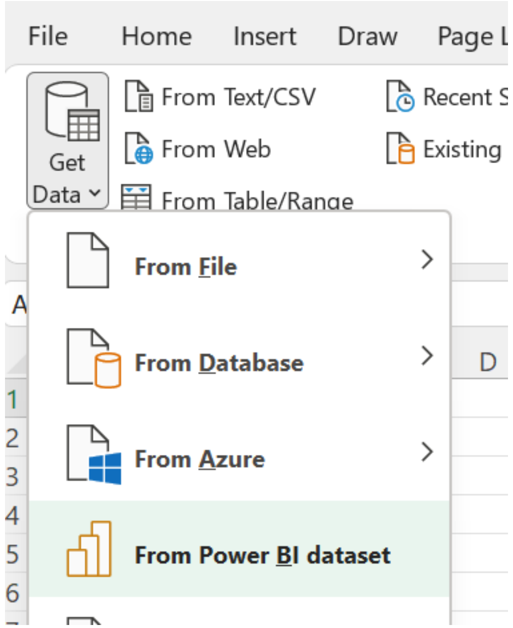
The dataset's sensitivity label "Confidential" will be applied to the new report.

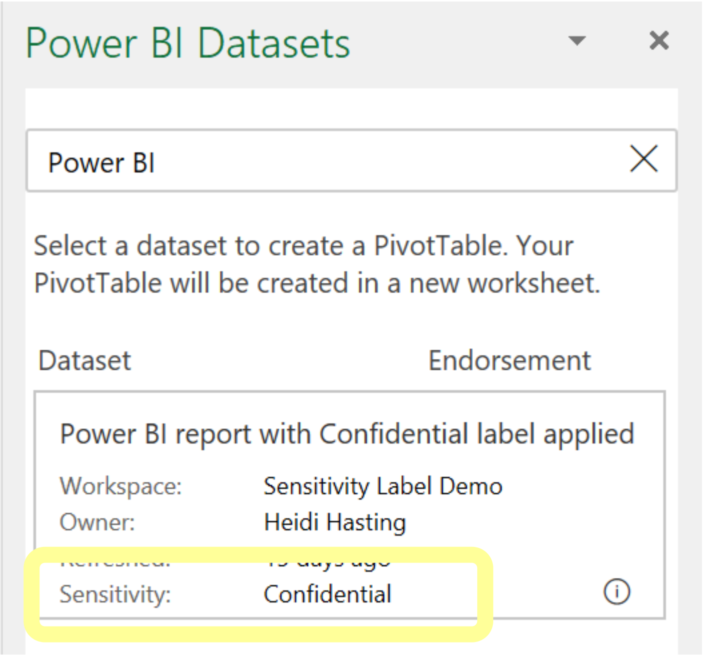
Save Cancel



Sensitivity Label Demo for datasource has labe | Confidential

Excel Analyse Power BI Dataset





Select a dataset to create a PivotTable. Your PivotTable will be created in a new worksheet.

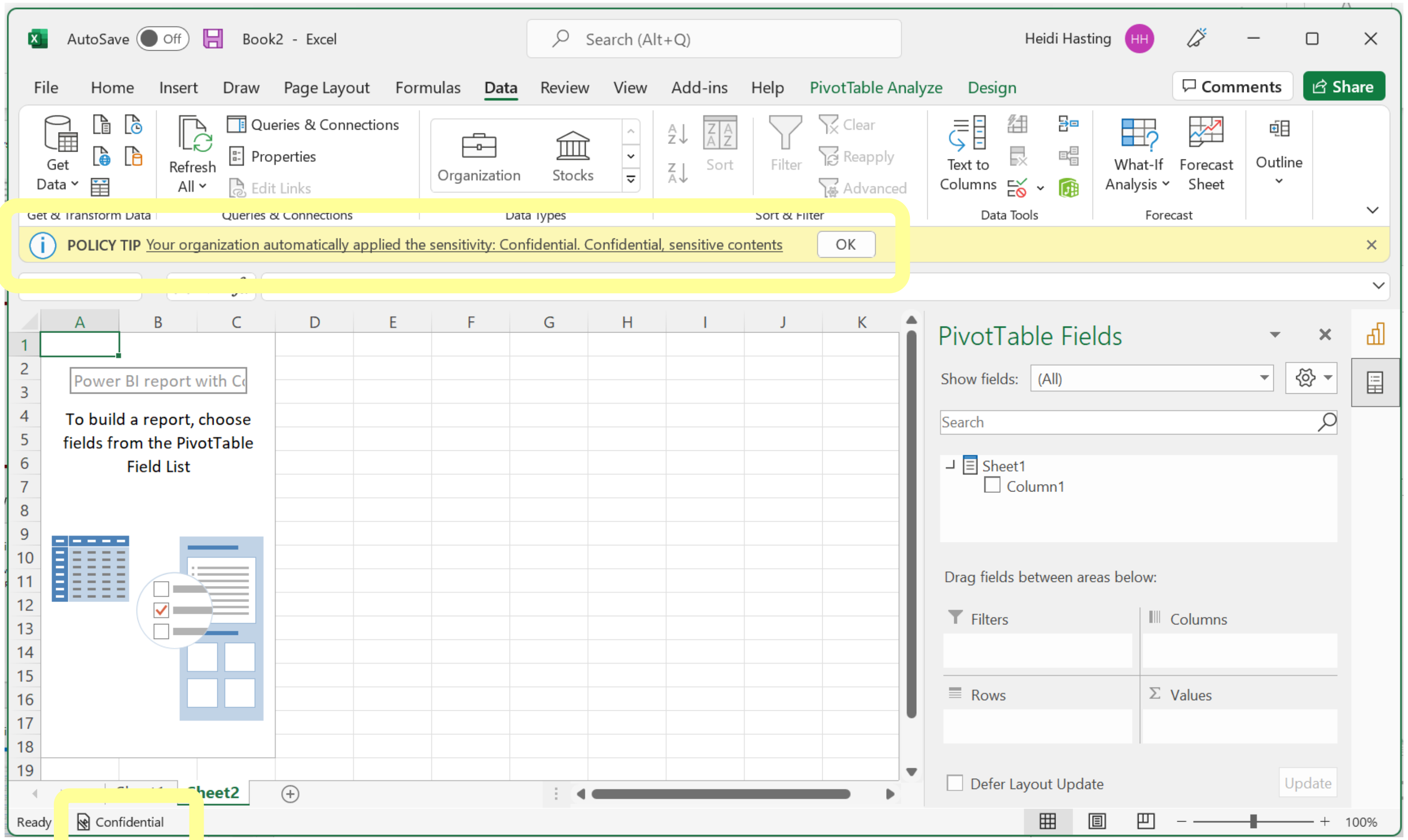
Dataset	Endorsement
Power BI report with Confidential label applied	

Workspace: Sensitivity Label Demo

Owner: Heidi Hasting

Sensitivity: Confidential

Excel continued…



POLICY TIP Your organization automatically applied the sensitivity: Confidential. Confidential, sensitive contents OK

To build a report, choose fields from the PivotTable Field List

Power BI – Gotcha’s

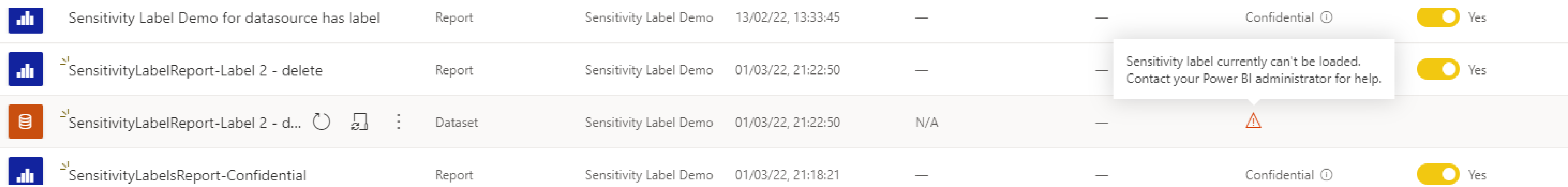
- Power BI report can have a sensitivity label applied the workspace access is all that’s required to view the report.

- Power BI Export to Excel – this is where the sensitivity label kicks in
  - If you don’t have access to the sensitivity label

- Data source sensitivity labels are inherited
  - Where there are multiple the label priority determines which one

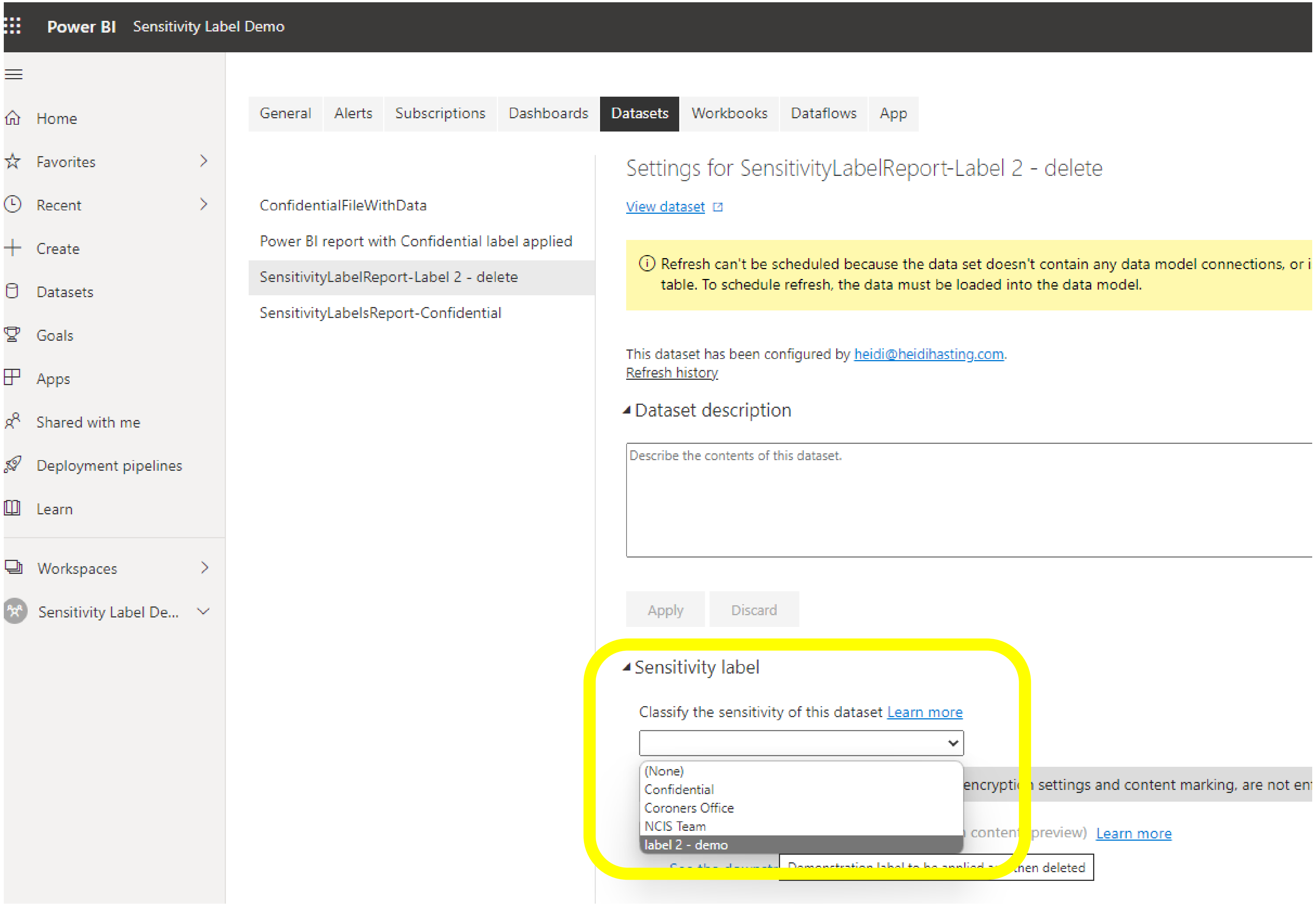
- B2B and multi-tenant scenarios not supported

Power BI – Gotcha's part 2



Sensitivity Label Demo for datasource has label	Report	Sensitivity Label Demo	13/02/22, 13:33:45	—	—	Confidential ⓘ	Yes
SensitivityLabelReport-Label 2 - delete	Report	Sensitivity Label Demo	01/03/22, 21:22:50	—	—		Yes
SensitivityLabelReport-Label 2 - d...	Dataset	Sensitivity Label Demo	01/03/22, 21:22:50	N/A	—	⚠	
SensitivityLabelsReport-Confidential	Report	Sensitivity Label Demo	01/03/22, 21:18:21	—	—	Confidential ⓘ	Yes

Sensitivity label currently can't be loaded. Contact your Power BI administrator for help.



Settings for SensitivityLabelReport-Label 2 - delete

View dataset

Refresh can't be scheduled because the data set doesn't contain any data model connections, or i
table. To schedule refresh, the data must be loaded into the data model.

This dataset has been configured by heidi@heidihasting.com.
Refresh history

Dataset description

Describe the contents of this dataset.

Sensitivity label

Classify the sensitivity of this dataset Learn more

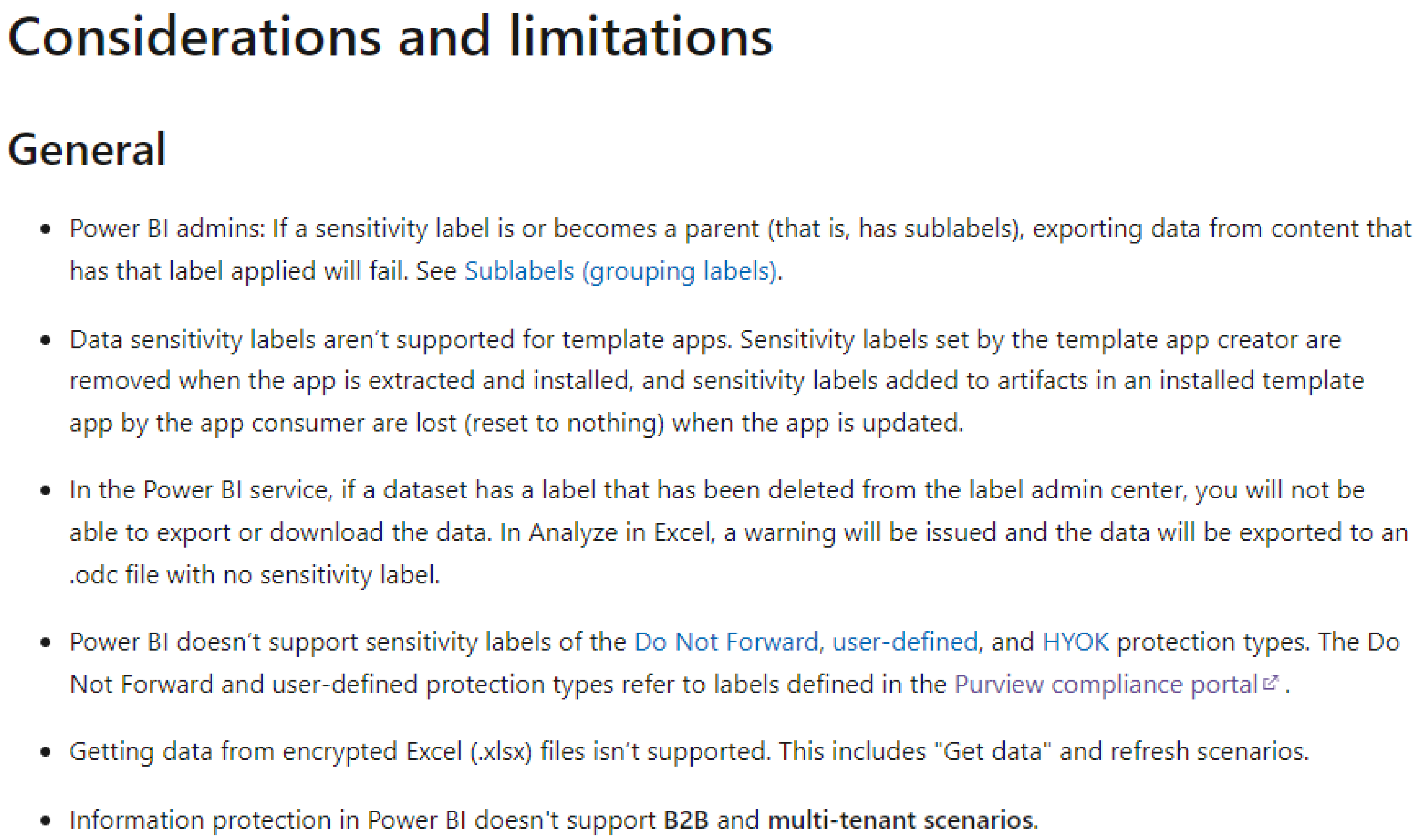
(None)
Confidential
Coroners Office
NCIS Team
label 2 - demo

encrypti settings and content marking, are not en

content preview) Learn more

then deleted

Other considerations – Microsoft Docs



Considerations and limitations

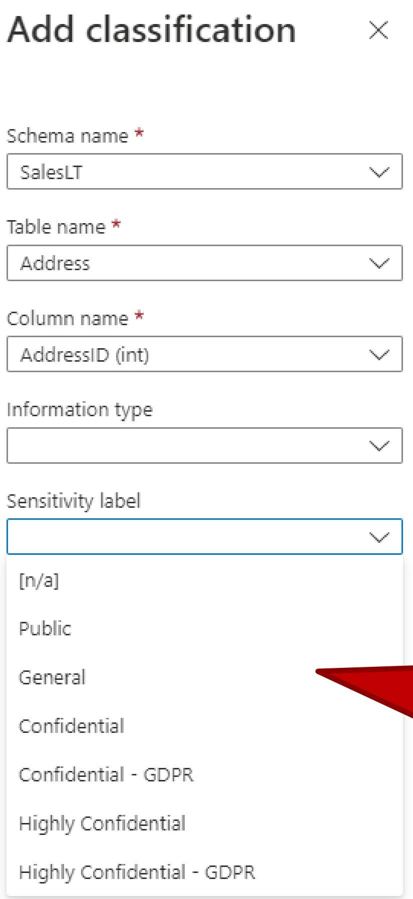
General

- Power BI admins: If a sensitivity label is or becomes a parent (that is, has sublabels), exporting data from content that has that label applied will fail. See Sublabels (grouping labels).
- Data sensitivity labels aren't supported for template apps. Sensitivity labels set by the template app creator are removed when the app is extracted and installed, and sensitivity labels added to artifacts in an installed template app by the app consumer are lost (reset to nothing) when the app is updated.
- In the Power BI service, if a dataset has a label that has been deleted from the label admin center, you will not be able to export or download the data. In Analyze in Excel, a warning will be issued and the data will be exported to an .odc file with no sensitivity label.
- Power BI doesn't support sensitivity labels of the Do Not Forward, user-defined, and HYOK protection types. The Do Not Forward and user-defined protection types refer to labels defined in the Purview compliance portal .
- Getting data from encrypted Excel (.xlsx) files isn't supported. This includes "Get data" and refresh scenarios.
- Information protection in Power BI doesn't support **B2B** and **multi-tenant scenarios**.

https://docs.microsoft.com/en-gb/power-bi/enterprise/service-security-sensitivity-label-overview#considerations-and-limitations

AZURE SQL

Azure SQL – add sensitivity label



Add classification

Schema name *
SalesLT

Table name *
Address

Column name *
AddressID (int)

Information type

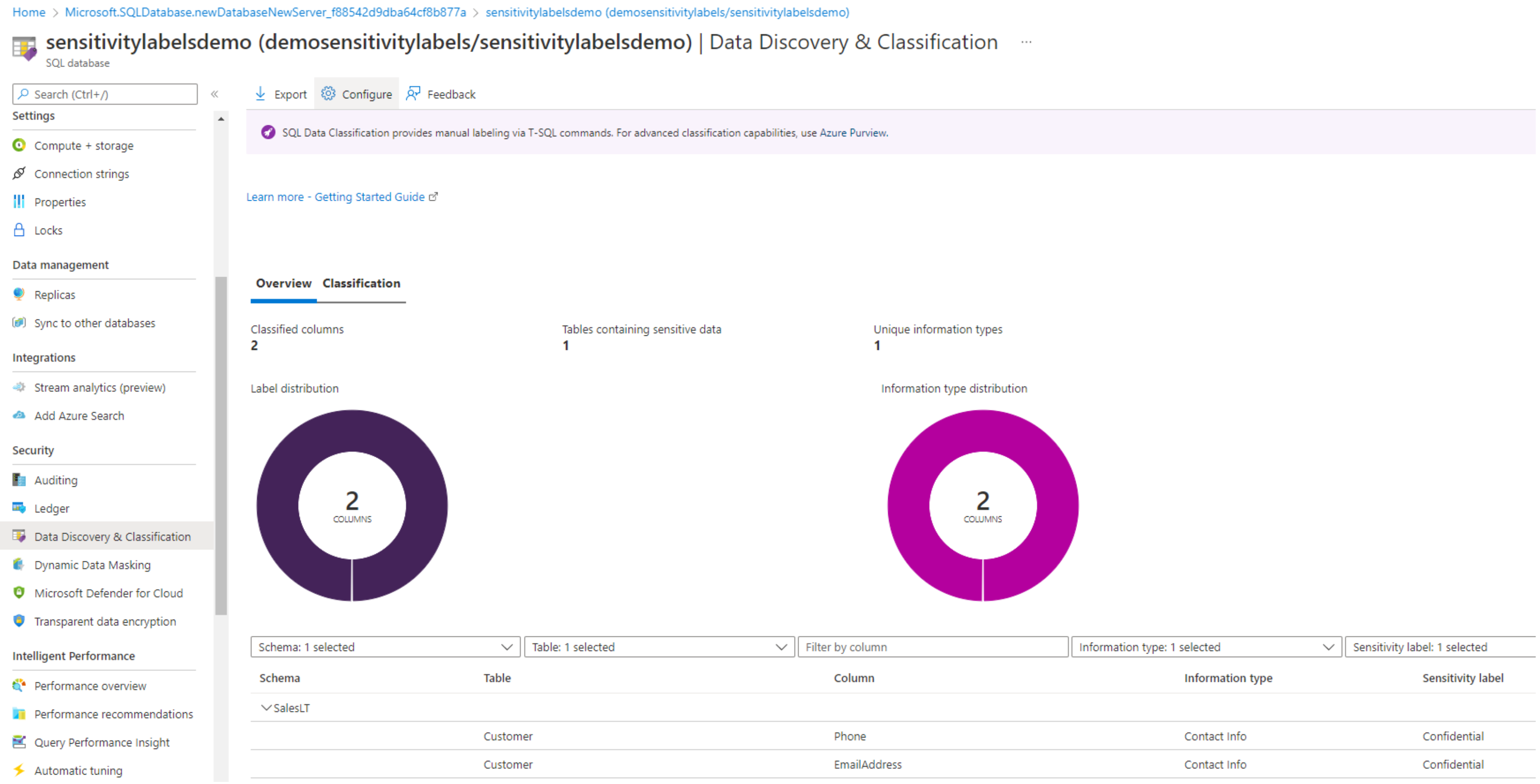
Sensitivity label

[n/a]
Public
General
Confidential
Confidential - GDPR
Highly Confidential
Highly Confidential - GDPR

Sensitivity List not the same as O365

- portal.azure
- Navigate to the Azure SQL resource
- Select Security > Data Discovery & Classification
- Select Classification
- Select Add classification

Azure SQL



sensitivitylabelsdemo (demosensitivitylabels/sensitivitylabelsdemo) | Data Discovery & Classification ...

SQL database

SQL Data Classification provides manual labeling via T-SQL commands. For advanced classification capabilities, use Azure Purview.

Learn more - Getting Started Guide

Classified columns
2

Tables containing sensitive data
1

Unique information types
1

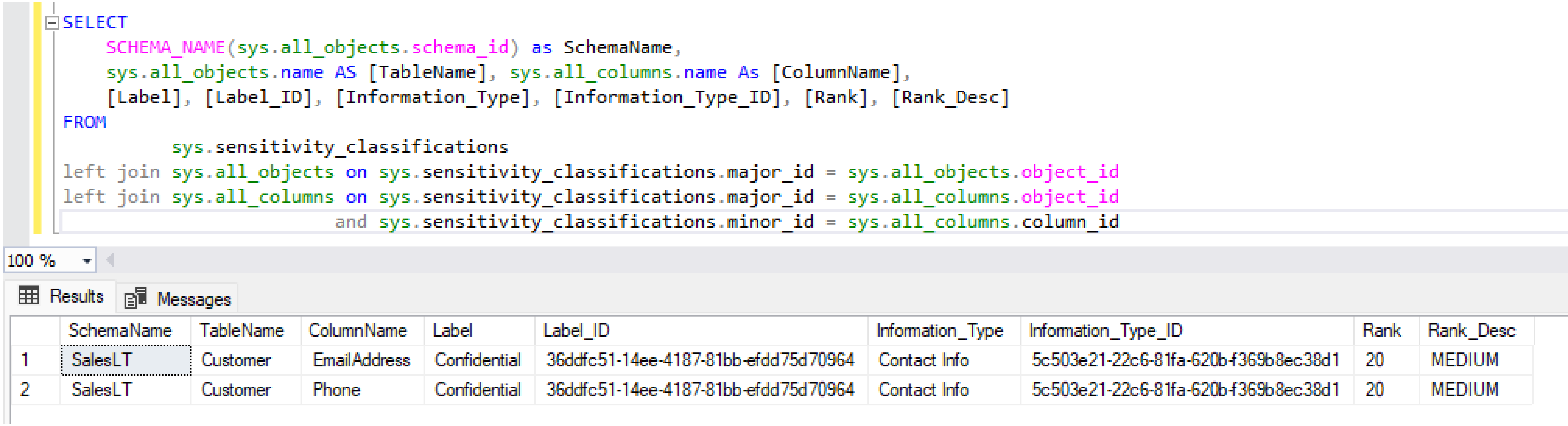
Label distribution

Information type distribution

Schema: 1 selected | Table: 1 selected | Filter by column | Information type: 1 selected | Sensitivity label: 1 selected

Schema	Table	Column	Information type	Sensitivity label
SalesLT				
	Customer	Phone	Contact Info	Confidential
	Customer	EmailAddress	Contact Info	Confidential

Azure SQL – view labels

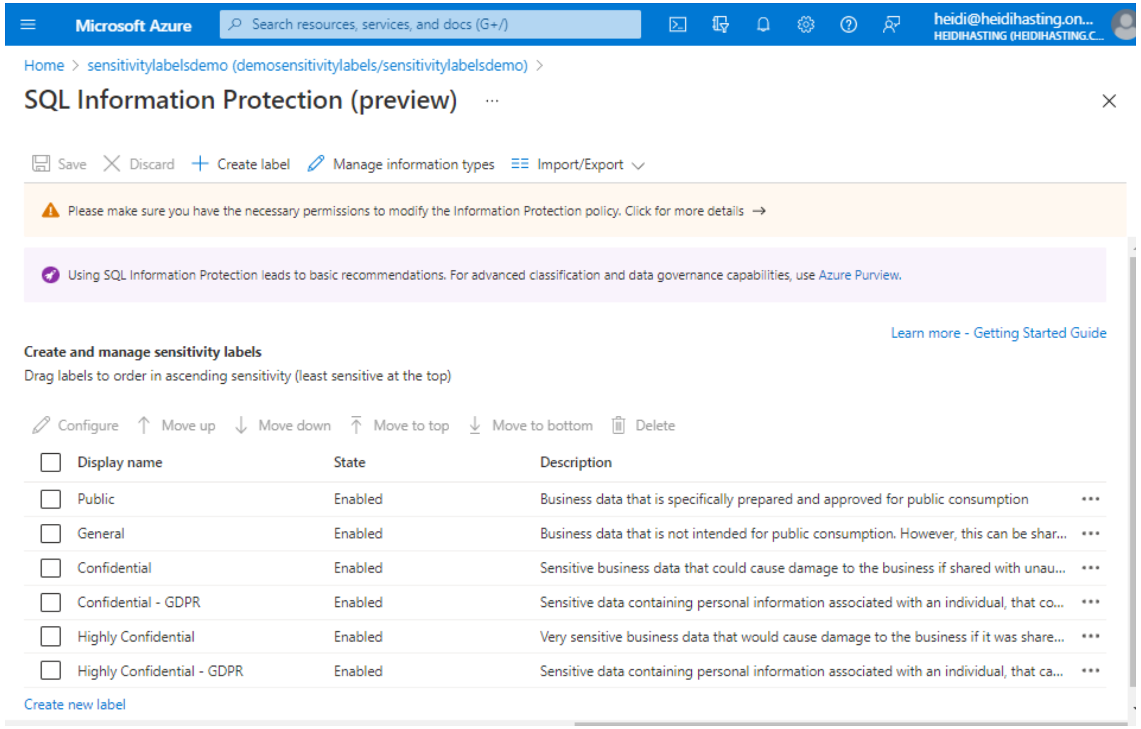


```
SELECT
    SCHEMA_NAME(sys.all_objects.schema_id) as SchemaName,
    sys.all_objects.name AS [TableName], sys.all_columns.name As [ColumnName],
    [Label], [Label_ID], [Information_Type], [Information_Type_ID], [Rank], [Rank_Desc]
FROM
          sys.sensitivity_classifications
left join sys.all_objects on sys.sensitivity_classifications.major_id = sys.all_objects.object_id
left join sys.all_columns on sys.sensitivity_classifications.major_id = sys.all_columns.object_id
                          and sys.sensitivity_classifications.minor_id = sys.all_columns.column_id
```

	SchemaName	TableName	ColumnName	Label	Label_ID	Information_Type	Information_Type_ID	Rank	Rank_Desc
1	SalesLT	Customer	EmailAddress	Confidential	36ddfc51-14ee-4187-81bb-efdd75d70964	Contact Info	5c503e21-22c6-81fa-620b-f369b8ec38d1	20	MEDIUM
2	SalesLT	Customer	Phone	Confidential	36ddfc51-14ee-4187-81bb-efdd75d70964	Contact Info	5c503e21-22c6-81fa-620b-f369b8ec38d1	20	MEDIUM

Azure SQL – add sensitivity labels

- portal.azure
- Navigate to the Azure SQL resource
- Select Security > Data Discovery & Classification
- Configure



Home > sensitivitylabelsdemo (demosensitivitylabels/sensitivitylabelsdemo) >

SQL Information Protection (preview) ···

Please make sure you have the necessary permissions to modify the Information Protection policy. Click for more details →

Using SQL Information Protection leads to basic recommendations. For advanced classification and data governance capabilities, use Azure Purview.

Learn more - Getting Started Guide

Create and manage sensitivity labels

Drag labels to order in ascending sensitivity (least sensitive at the top)

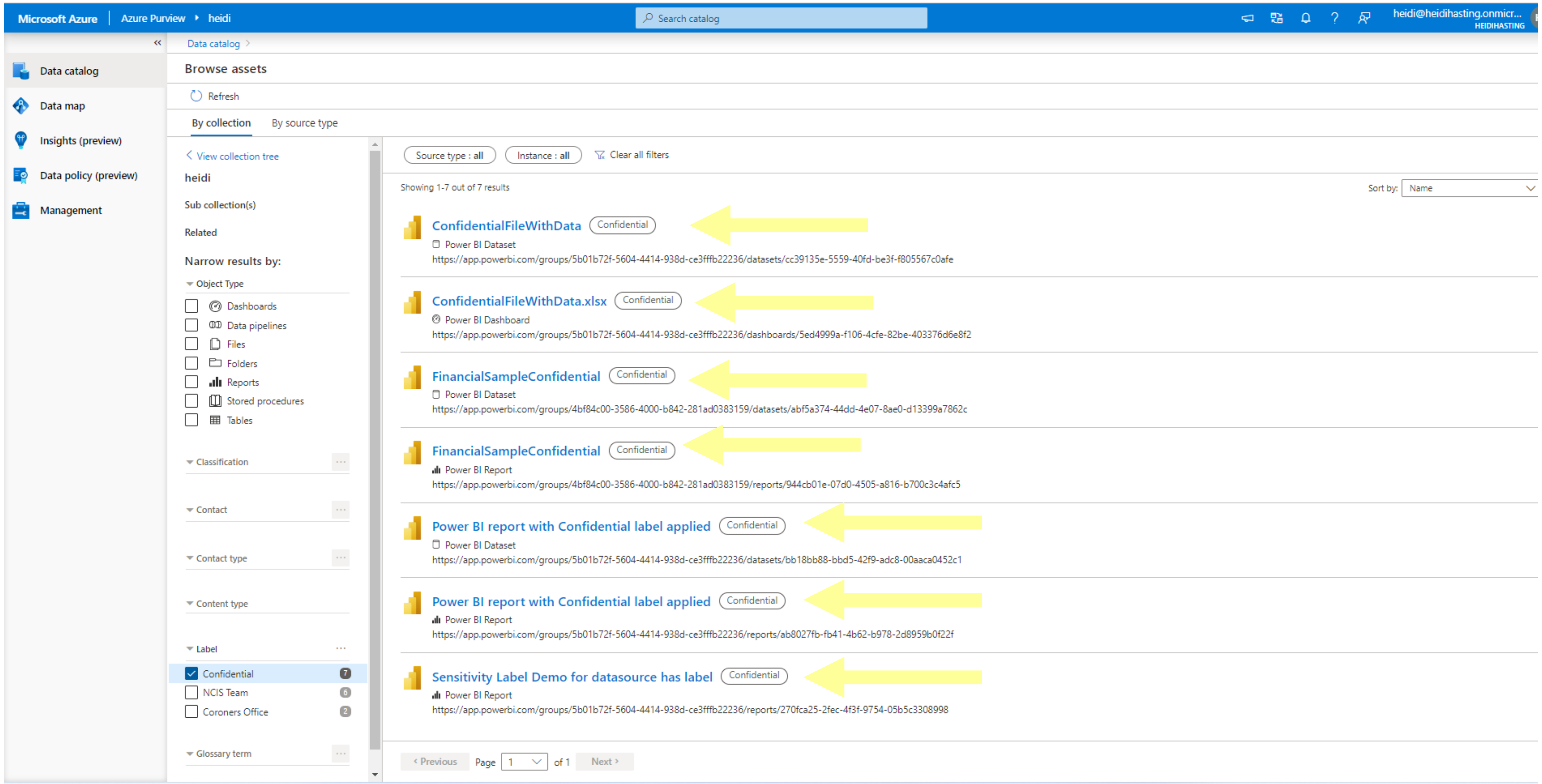
□	Display name	State	Description	
□	Public	Enabled	Business data that is specifically prepared and approved for public consumption	···
□	General	Enabled	Business data that is not intended for public consumption. However, this can be shar...	···
□	Confidential	Enabled	Sensitive business data that could cause damage to the business if shared with unau...	···
□	Confidential - GDPR	Enabled	Sensitive data containing personal information associated with an individual, that co...	···
□	Highly Confidential	Enabled	Very sensitive business data that would cause damage to the business if it was share...	···
□	Highly Confidential - GDPR	Enabled	Sensitive data containing personal information associated with an individual, that ca...	···

Create new label

Azure Purview (PREVIEW)

- Viewing Sensitivity Labels
- Automatically applying sensitivity labels

Azure Purview Data catalog



Showing 1-7 out of 7 results

ConfidentialFileWithData Confidential
Power BI Dataset
https://app.powerbi.com/groups/5b01b72f-5604-4414-938d-ce3fffb22236/datasets/cc39135e-5559-40fd-be3f-f805567c0afe

ConfidentialFileWithData.xlsx Confidential
Power BI Dashboard
https://app.powerbi.com/groups/5b01b72f-5604-4414-938d-ce3fffb22236/dashboards/5ed4999a-f106-4cfe-82be-403376d6e8f2

FinancialSampleConfidential Confidential
Power BI Dataset
https://app.powerbi.com/groups/4bf84c00-3586-4000-b842-281ad0383159/datasets/abf5a374-44dd-4e07-8ae0-d13399a7862c

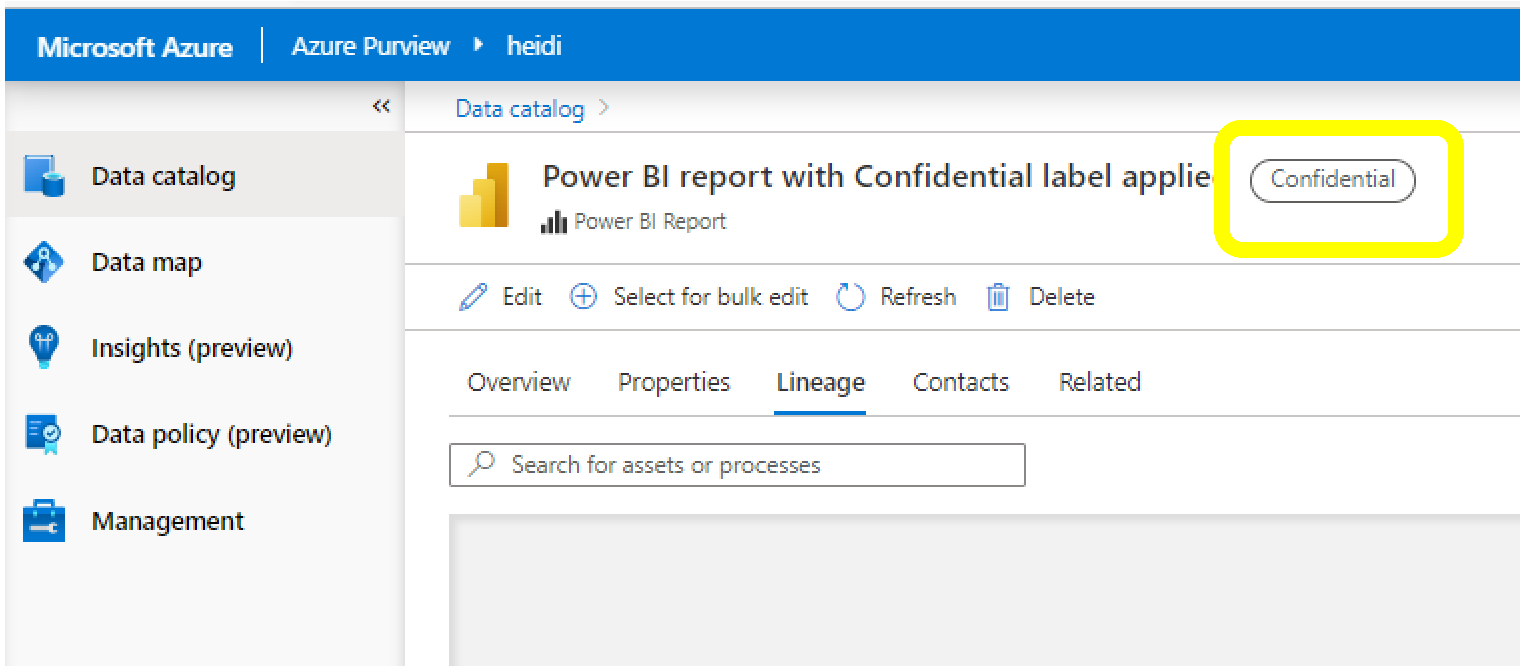
FinancialSampleConfidential Confidential
Power BI Report
https://app.powerbi.com/groups/4bf84c00-3586-4000-b842-281ad0383159/reports/944cb01e-07d0-4505-a816-b700c3c4afc5

Power BI report with Confidential label applied Confidential
Power BI Dataset
https://app.powerbi.com/groups/5b01b72f-5604-4414-938d-ce3fffb22236/datasets/bb18bb88-bbd5-42f9-adc8-00aaca0452c1

Power BI report with Confidential label applied Confidential
Power BI Report
https://app.powerbi.com/groups/5b01b72f-5604-4414-938d-ce3fffb22236/reports/ab8027fb-fb41-4b62-b978-2d8959b0f22f

Sensitivity Label Demo for datasource has label Confidential
Power BI Report
https://app.powerbi.com/groups/5b01b72f-5604-4414-938d-ce3fffb22236/reports/270fca25-2fec-4f3f-9754-05b5c3308998

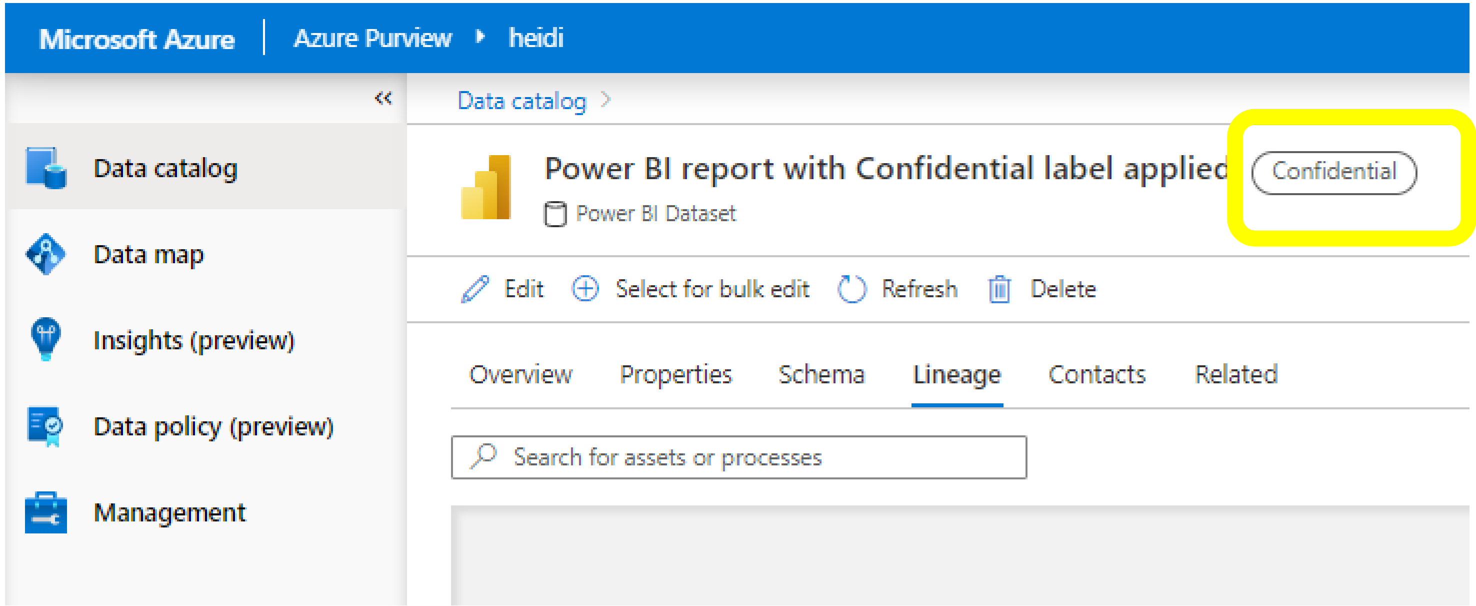
Power BI report shows sensitivity label



Power BI report with Confidential label applie

Power BI Report

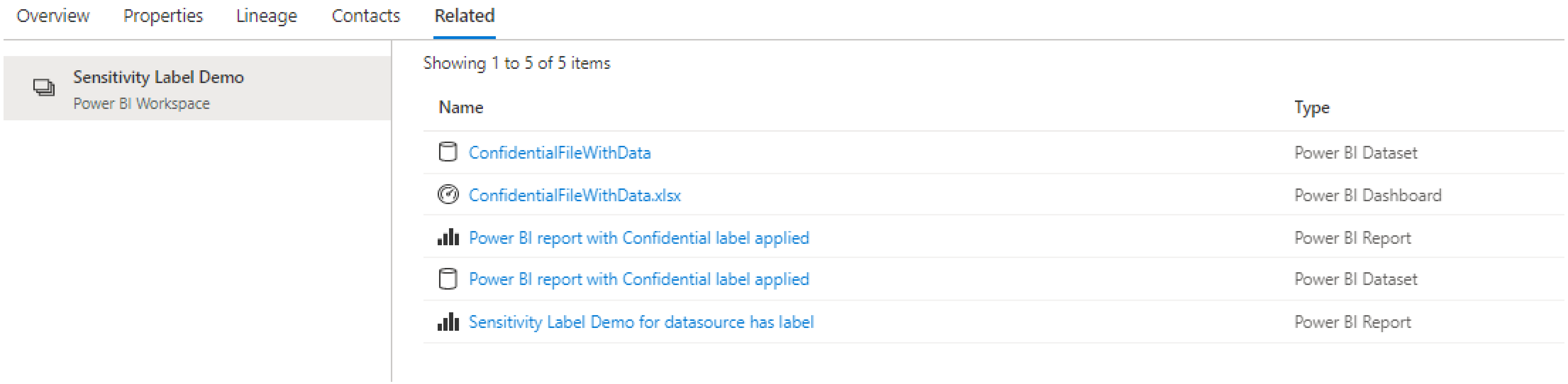
Power BI dataset shows sensitivity label



Power BI report with Confidential label applied Confidential

Power BI Dataset

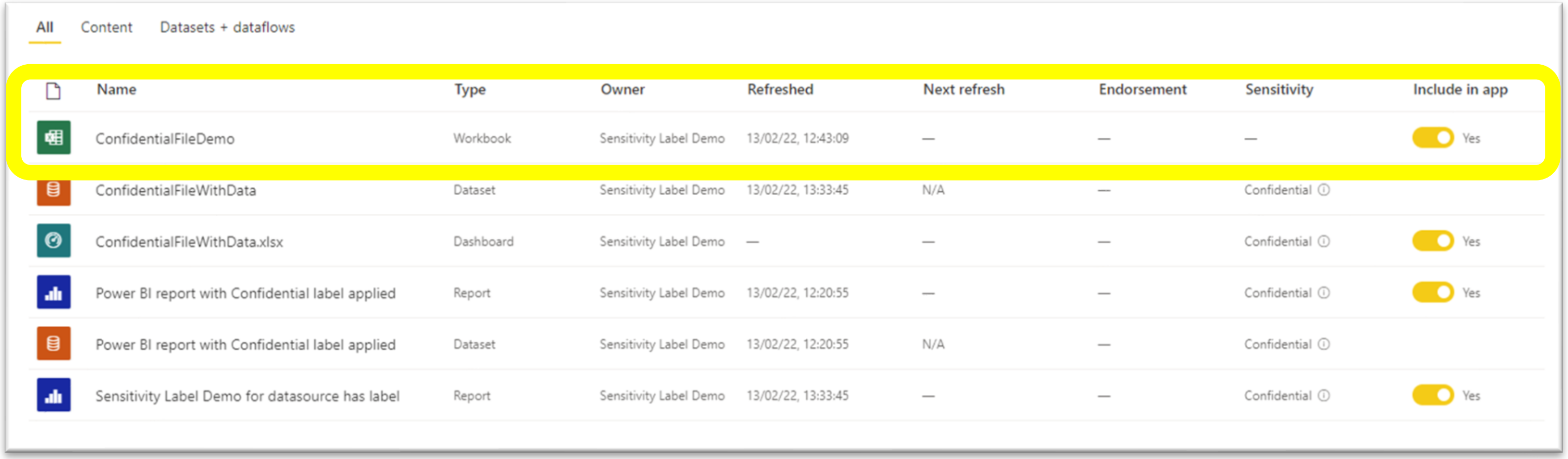
Power BI Excel Workbook – N/A in Purview



Sensitivity Label Demo
Power BI Workspace

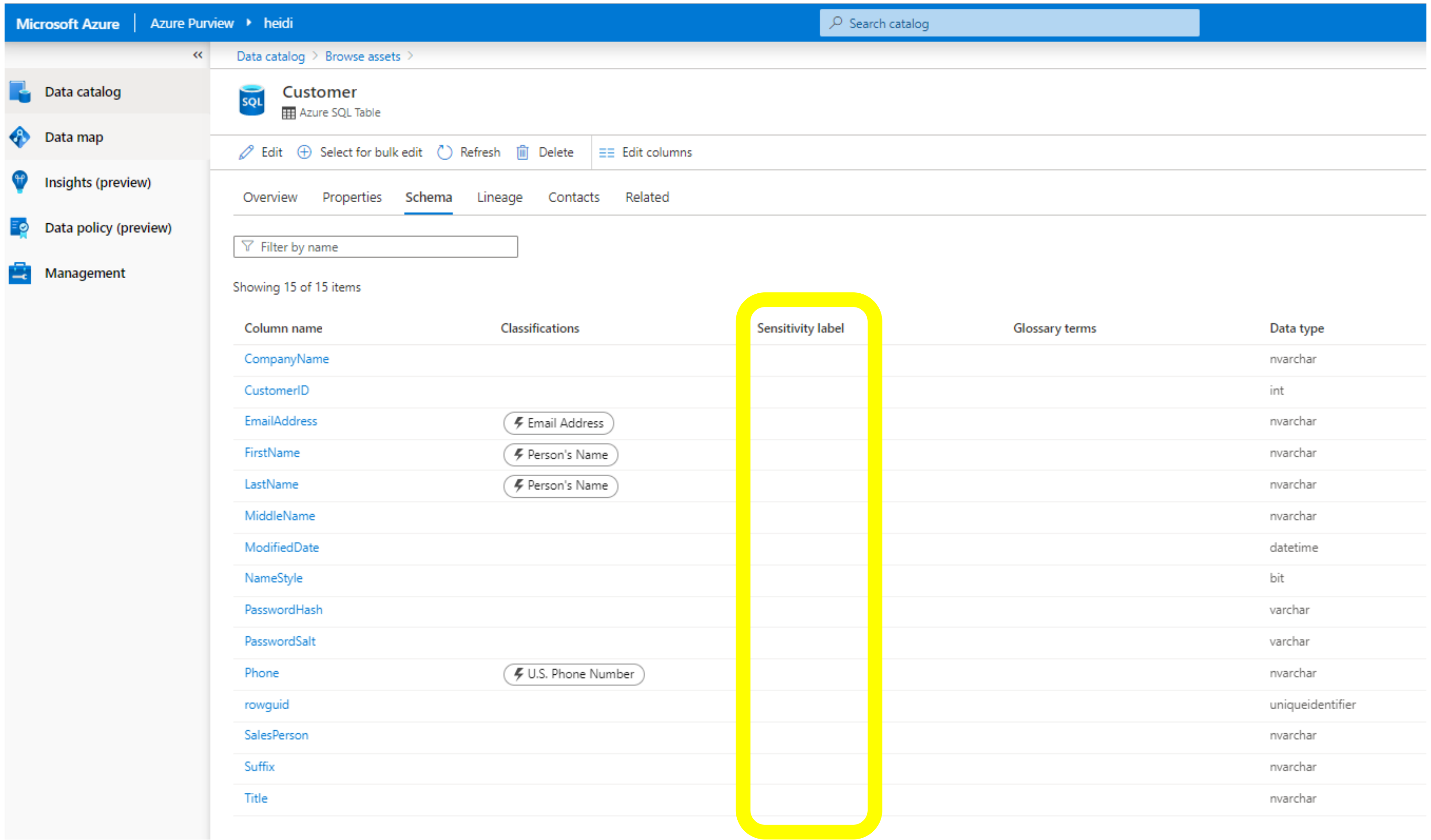
Showing 1 to 5 of 5 items

Name	Type
ConfidentialFileWithData	Power BI Dataset
ConfidentialFileWithData.xlsx	Power BI Dashboard
Power BI report with Confidential label applied	Power BI Report
Power BI report with Confidential label applied	Power BI Dataset
Sensitivity Label Demo for datasource has label	Power BI Report



Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Include in app
ConfidentialFileDemo	Workbook	Sensitivity Label Demo	13/02/22, 12:43:09	—	—	—	Yes
ConfidentialFileWithData	Dataset	Sensitivity Label Demo	13/02/22, 13:33:45	N/A	—	Confidential ⓘ	
ConfidentialFileWithData.xlsx	Dashboard	Sensitivity Label Demo	—	—	—	Confidential ⓘ	Yes
Power BI report with Confidential label applied	Report	Sensitivity Label Demo	13/02/22, 12:20:55	—	—	Confidential ⓘ	Yes
Power BI report with Confidential label applied	Dataset	Sensitivity Label Demo	13/02/22, 12:20:55	N/A	—	Confidential ⓘ	
Sensitivity Label Demo for datasource has label	Report	Sensitivity Label Demo	13/02/22, 13:33:45	—	—	Confidential ⓘ	Yes

Azure SQL

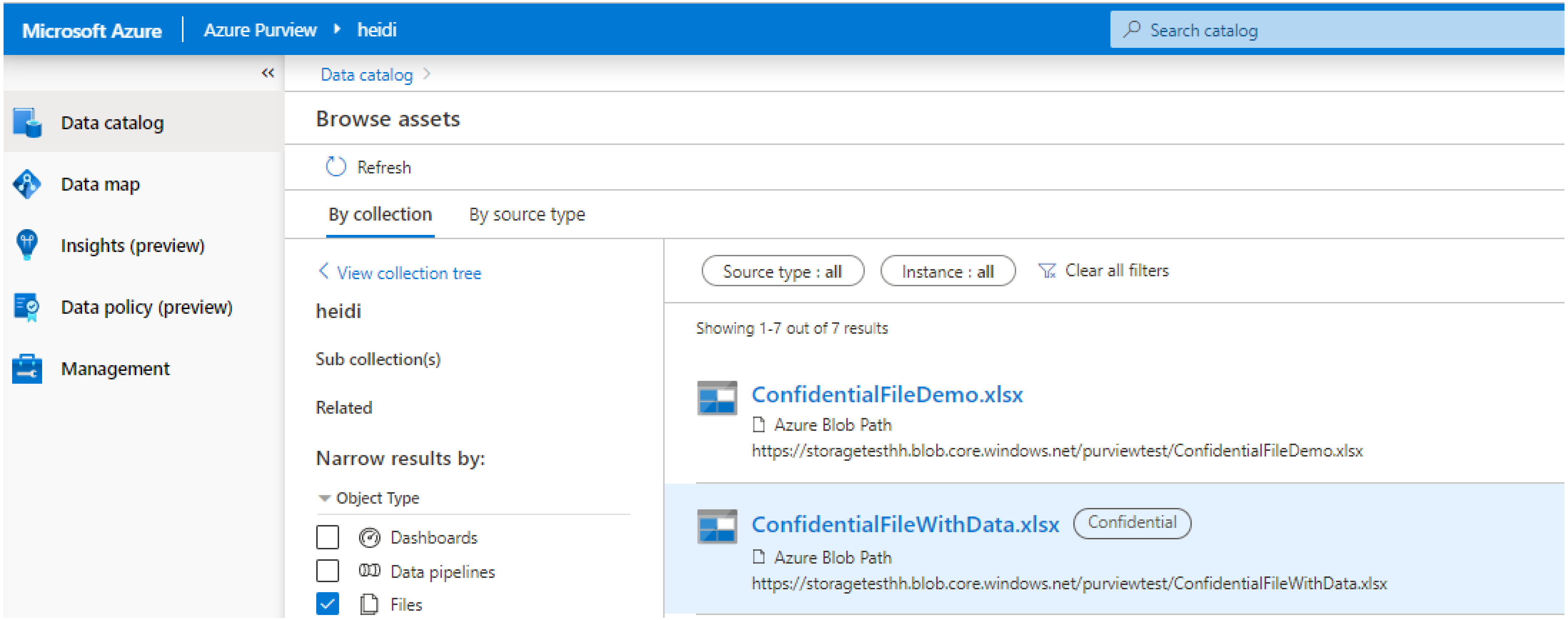


Customer
Azure SQL Table

Showing 15 of 15 items

Column name	Classifications	Sensitivity label	Glossary terms	Data type
CompanyName				nvarchar
CustomerID				int
EmailAddress	Email Address			nvarchar
FirstName	Person's Name			nvarchar
LastName	Person's Name			nvarchar
MiddleName				nvarchar
ModifiedDate				datetime
NameStyle				bit
PasswordHash				varchar
PasswordSalt				varchar
Phone	U.S. Phone Number			nvarchar
rowguid				uniqueidentifier
SalesPerson				nvarchar
Suffix				nvarchar
Title				nvarchar

Azure Blob – files with sensitivity label



Browse assets

heidi

Sub collection(s)

Related

Narrow results by:

Object Type

☐ Dashboards

☐ Data pipelines

☑ Files

Source type : all

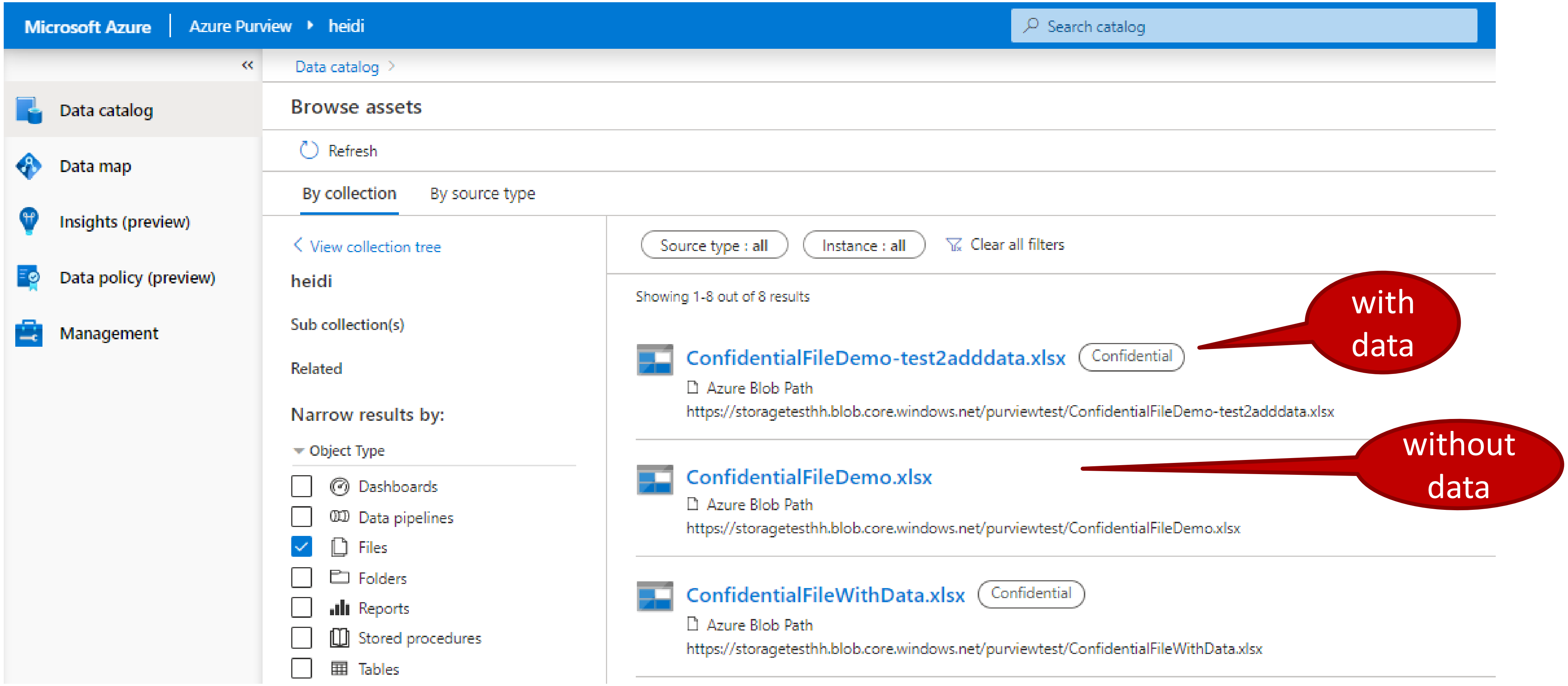
Instance : all

Clear all filters

Showing 1-7 out of 7 results

ConfidentialFileDemo.xlsx
Azure Blob Path
https://storagetesthh.blob.core.windows.net/purviewtest/ConfidentialFileDemo.xlsx

ConfidentialFileWithData.xlsx Confidential
Azure Blob Path
https://storagetesthh.blob.core.windows.net/purviewtest/ConfidentialFileWithData.xlsx



Data catalog >

Browse assets

< View collection tree

heidi

Sub collection(s)

Related

Narrow results by:

Object Type

- □ Dashboards
- □ Data pipelines
- ☑ Files
- □ Folders
- □ Reports
- □ Stored procedures
- □ Tables

Source type : all

Instance : all

Clear all filters

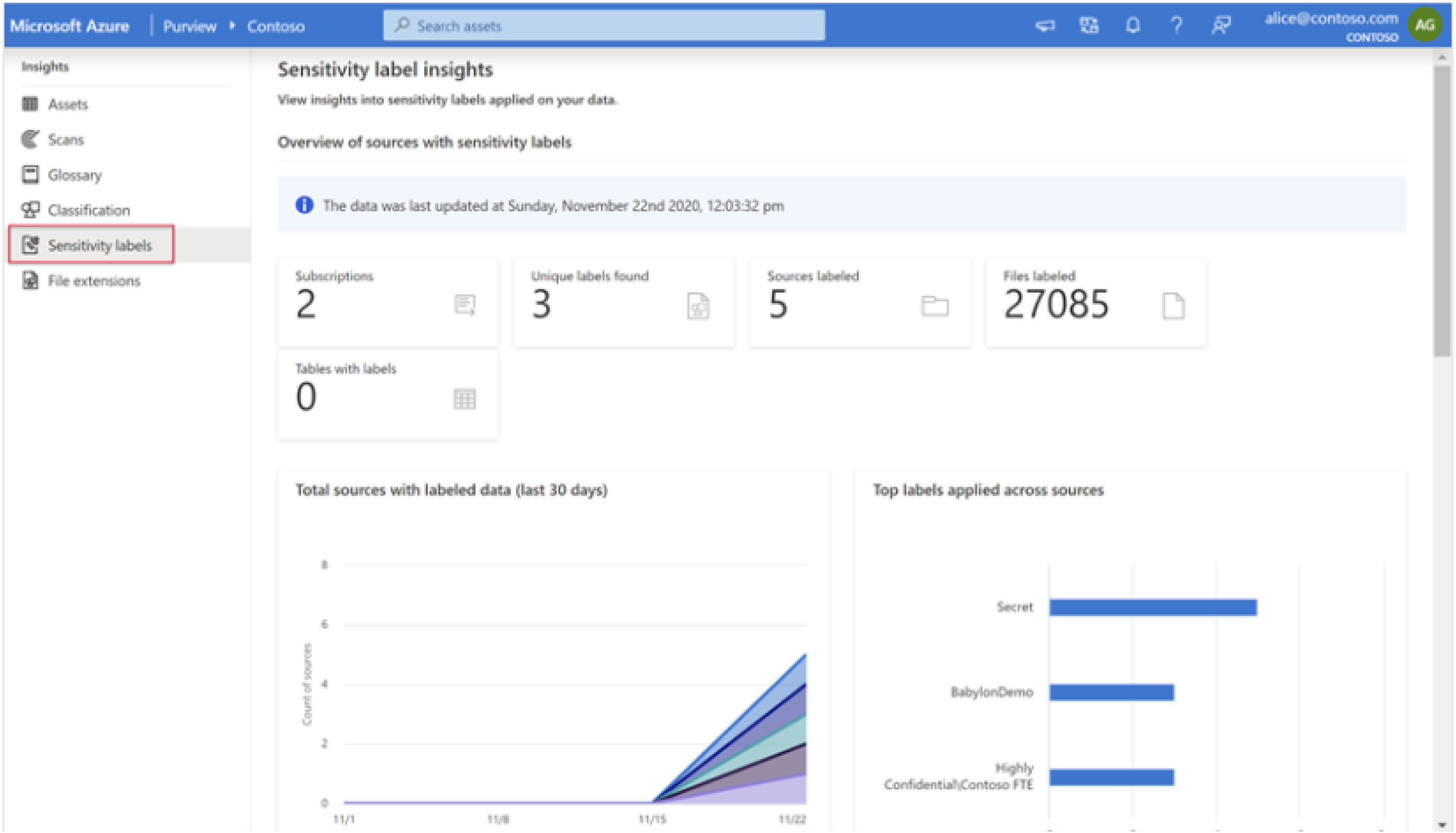
Showing 1-8 out of 8 results

ConfidentialFileDemo-test2adddata.xlsx Confidential
Azure Blob Path
https://storagetesthh.blob.core.windows.net/purviewtest/ConfidentialFileDemo-test2adddata.xlsx

ConfidentialFileDemo.xlsx
Azure Blob Path
https://storagetesthh.blob.core.windows.net/purviewtest/ConfidentialFileDemo.xlsx

ConfidentialFileWithData.xlsx Confidential
Azure Blob Path
https://storagetesthh.blob.core.windows.net/purviewtest/ConfidentialFileWithData.xlsx

Insights



Sensitivity label insights

View insights into sensitivity labels applied on your data.

Overview of sources with sensitivity labels

The data was last updated at Sunday, November 22nd 2020, 12:03:32 pm

Subscriptions 2

Unique labels found 3

Sources labeled 5

Files labeled 27085

Tables with labels 0

Total sources with labeled data (last 30 days)

Top labels applied across sources

https://docs.microsoft.com/en-us/azure/purview/sensitivity-insights
#:~:text=%20To%20view%20sensitivity%20labeling%20insights%3A%20%201,the%20Purview%20Sensitivity%20labeling%20insights%20report.%0ANote%0AIf...%20More%20

Resources

- Licensing requirements for sensitivity labels
  - https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance#information-protection-sensitivity-labeling

- Azure SQL
  - https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview
  - https://docs.microsoft.com/en-us/sql/relational-databases/system-catalog-views/sys-sensitivity-classifications-transact-sql?view=sql-server-ver15

- Azure Purview auto labelling
  - Info types https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-entity-definitions?view=o365-worldwide
  - https://docs.microsoft.com/en-us/azure/purview/how-to-automatically-label-your-content#autolabeling-for-schematized-data-assets

Recap

- Sensitivity label maintenance and management is through O365 Compliance
- We looked at how the sensitivity labels appear in
  - Power BI
  - Office
  - Azure SQL
  - Azure Purview
- Couple of gotchas

Thank you to our Sponsors!!!!

COZYROC™
Go to the next level

BALEEN DATA
A Branded Division of Geffen Mesher

smart
casual
datadesign

Microsoft Azure

redgate

solarwinds

ADVANTIS GLOBAL
Connecting People to Opportunity

SQL SATURDAY
2022 Oregon & SW Washington

Thank you

Heidi Hasting

@HeidiHasting

www.heidihasting.com