Microsoft Security

Purview
Data Protection and Security for Power BI for GCC

Moderator :
Leo Ramirez - Principal Technical Specialist, Microsoft

Speakers
Bhavana Bhatia – Sr Technical Specialist, Microsoft
Cyrus Christian – Sr Technical Specialist, Microsoft

Protect your data in Power BI

Microsoft Purview

Information Protection

Classify and protect your data from breaches and exfiltration with sensitivity labels.

Capabilities include:

- Classify and label sensitive Power BI data
- Enforce governance policies even when Power BI content is exported to supported export formats

Microsoft Purview

Data loss prevention

Reduce the risk of sensitive business data leakage from Power BI.

Capabilities include:

- Evaluate all semantic models within the workspaces
- Detect when sensitive data is uploaded into your Premium capacities
- See customized policy tip when semantic model identified as sensitive

Microsoft Defender for Cloud Apps

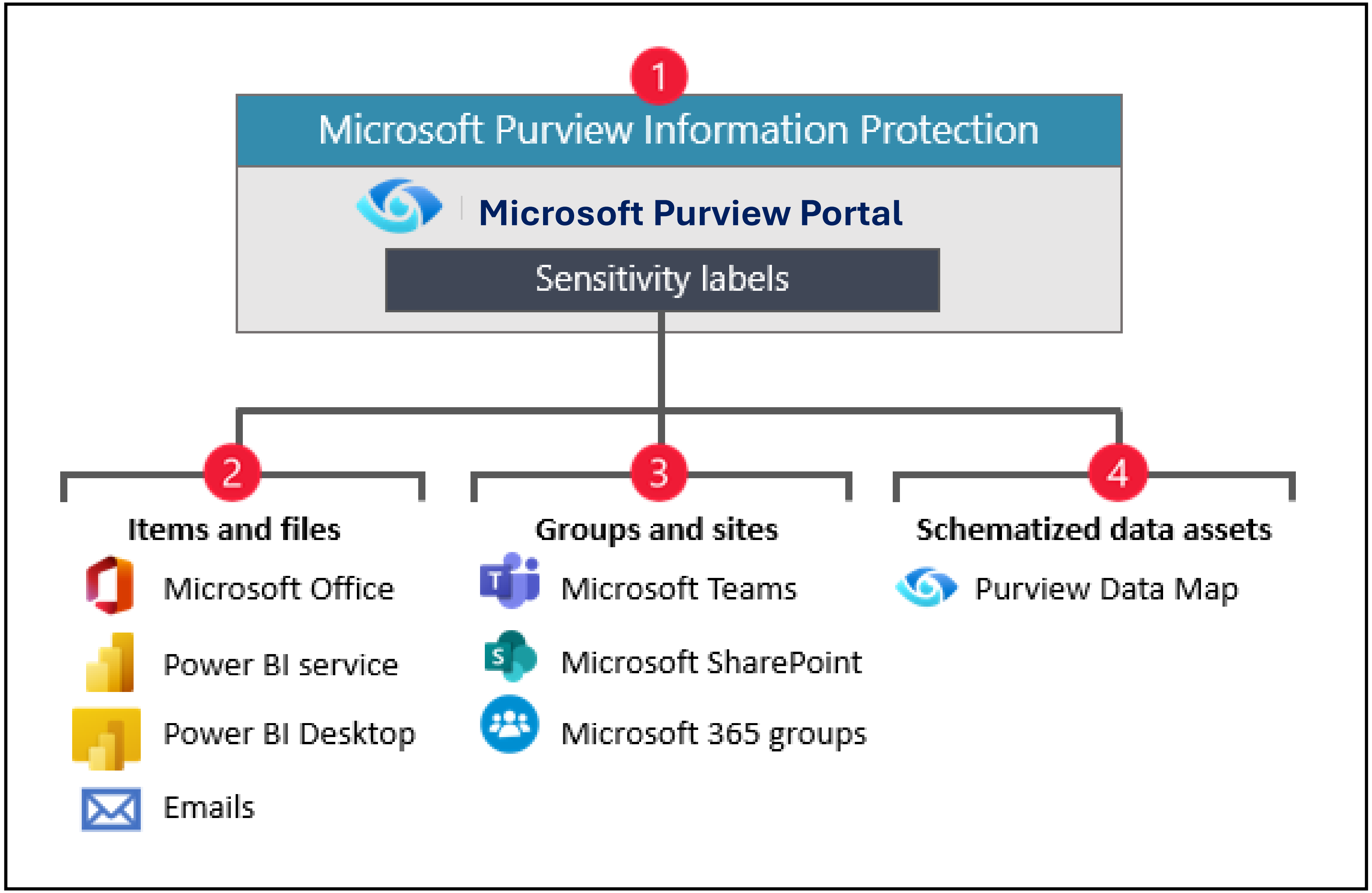
Security

Protect your Power BI reports, data, and services from unintended leaks or breaches.

Capabilities include:

- Create conditional access policies by using real-time session controls in Microsoft Entra ID
- Security admin capabilities to monitor user access and activity
- Perform real-time risk analysis

Purview Information Protection for Power BI



1 Microsoft Purview Information Protection

Microsoft Purview Portal

Sensitivity labels

2 **Items and files**

- Microsoft Office
- Power BI service
- Power BI Desktop
- Emails

3 **Groups and sites**

- Microsoft Teams
- Microsoft SharePoint
- Microsoft 365 groups

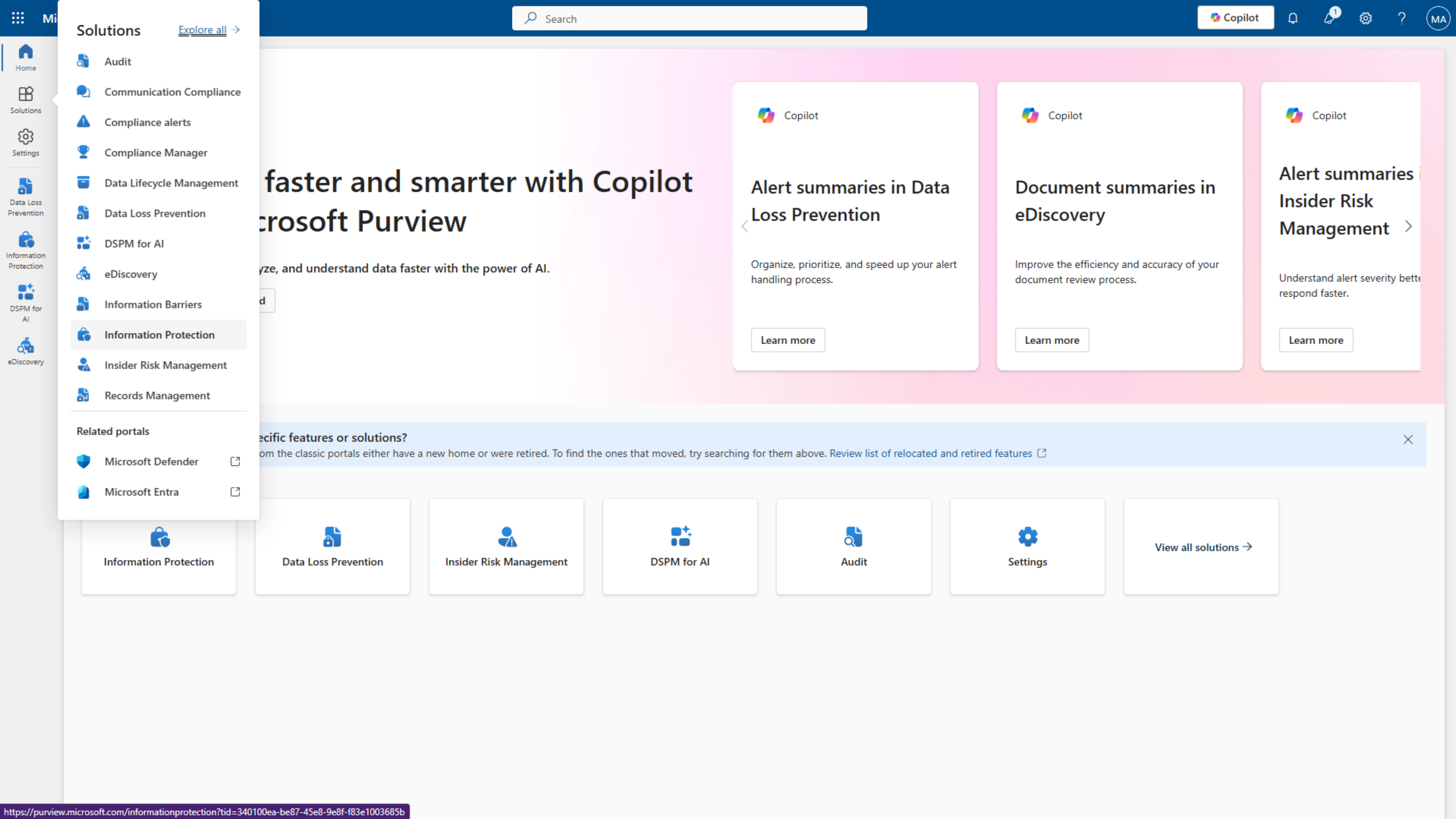
4 **Schematized data assets**

- Purview Data Map

Sensitivity Labels

- Sensitivity labels are part of the Information protection framework
- Only one label can be assigned to each item
- Sensitivity label has the following purposes.
  - **Classification:** It provides a classification for describing the sensitivity level.
  - **User education and awareness:** It helps users understand how to appropriately work with the content.
  - **Policies:** It forms the basis for applying and enforcing policies and DLP.

Create Sensitivity Labels



faster and smarter with Copilot
crosoft Purview

yze, and understand data faster with the power of AI.

Alert summaries in Data Loss Prevention

Organize, prioritize, and speed up your alert handling process.

Document summaries in eDiscovery

Improve the efficiency and accuracy of your document review process.

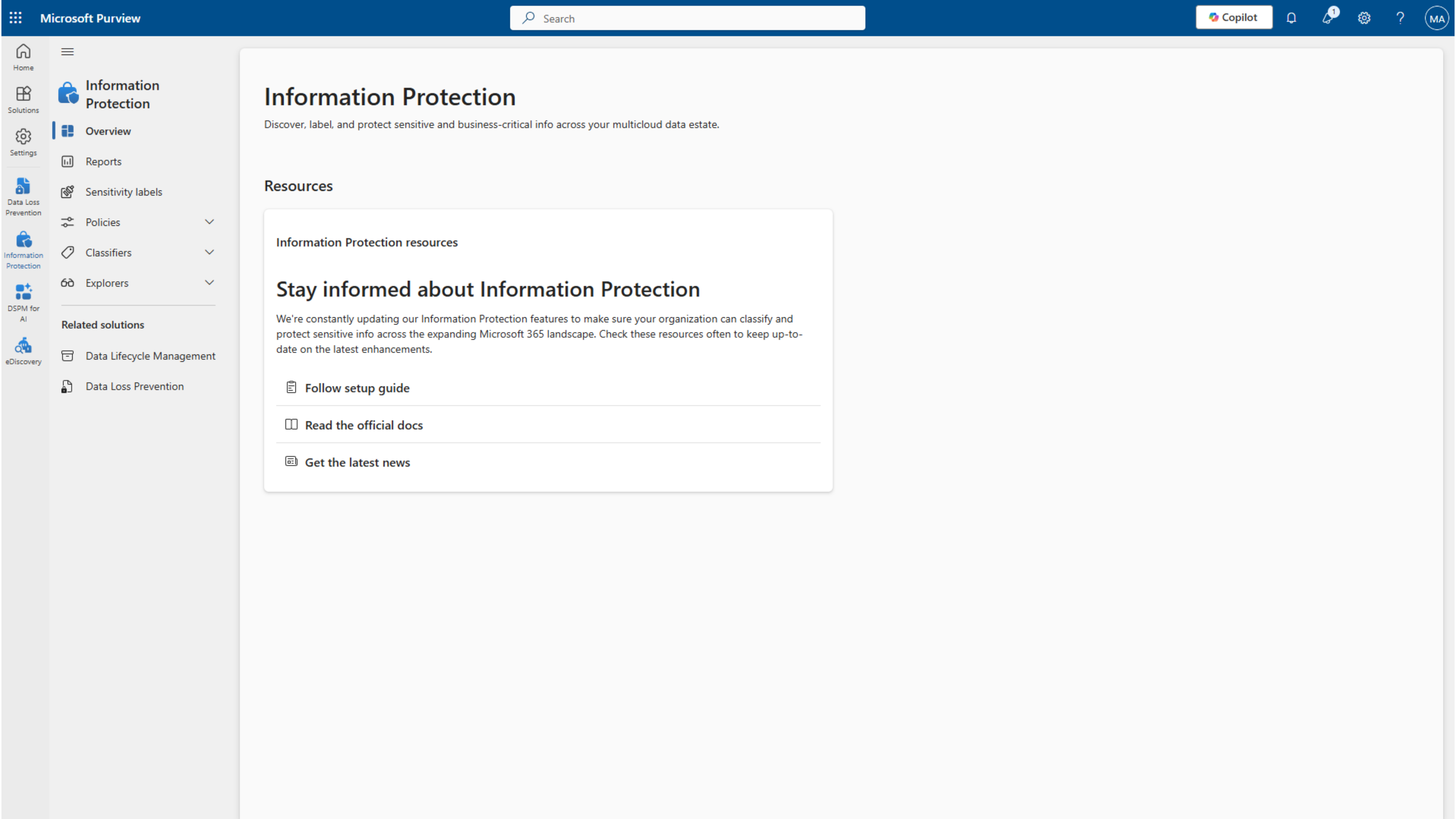
Alert summaries i Insider Risk Management

Understand alert severity bette respond faster.

ecific features or solutions?

om the classic portals either have a new home or were retired. To find the ones that moved, try searching for them above. Review list of relocated and retired features

https://purview.microsoft.com/informationprotection?tid=340100ea-be87-45e8-9e8f-f83e1003685b



Information Protection

Discover, label, and protect sensitive and business-critical info across your multicloud data estate.

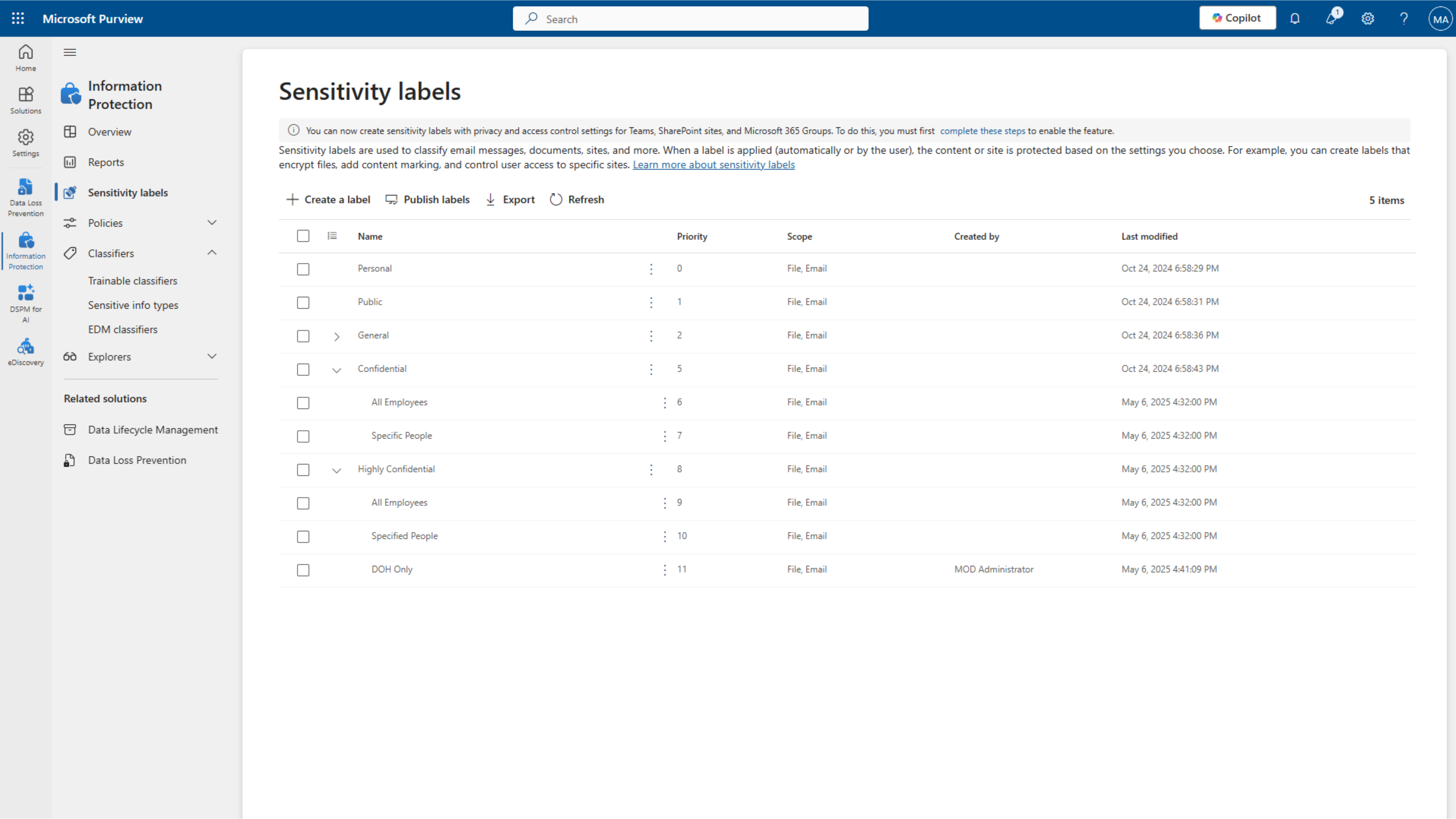
Resources

Information Protection resources

Stay informed about Information Protection

We're constantly updating our Information Protection features to make sure your organization can classify and protect sensitive info across the expanding Microsoft 365 landscape. Check these resources often to keep up-to-date on the latest enhancements.

- Follow setup guide
- Read the official docs
- Get the latest news

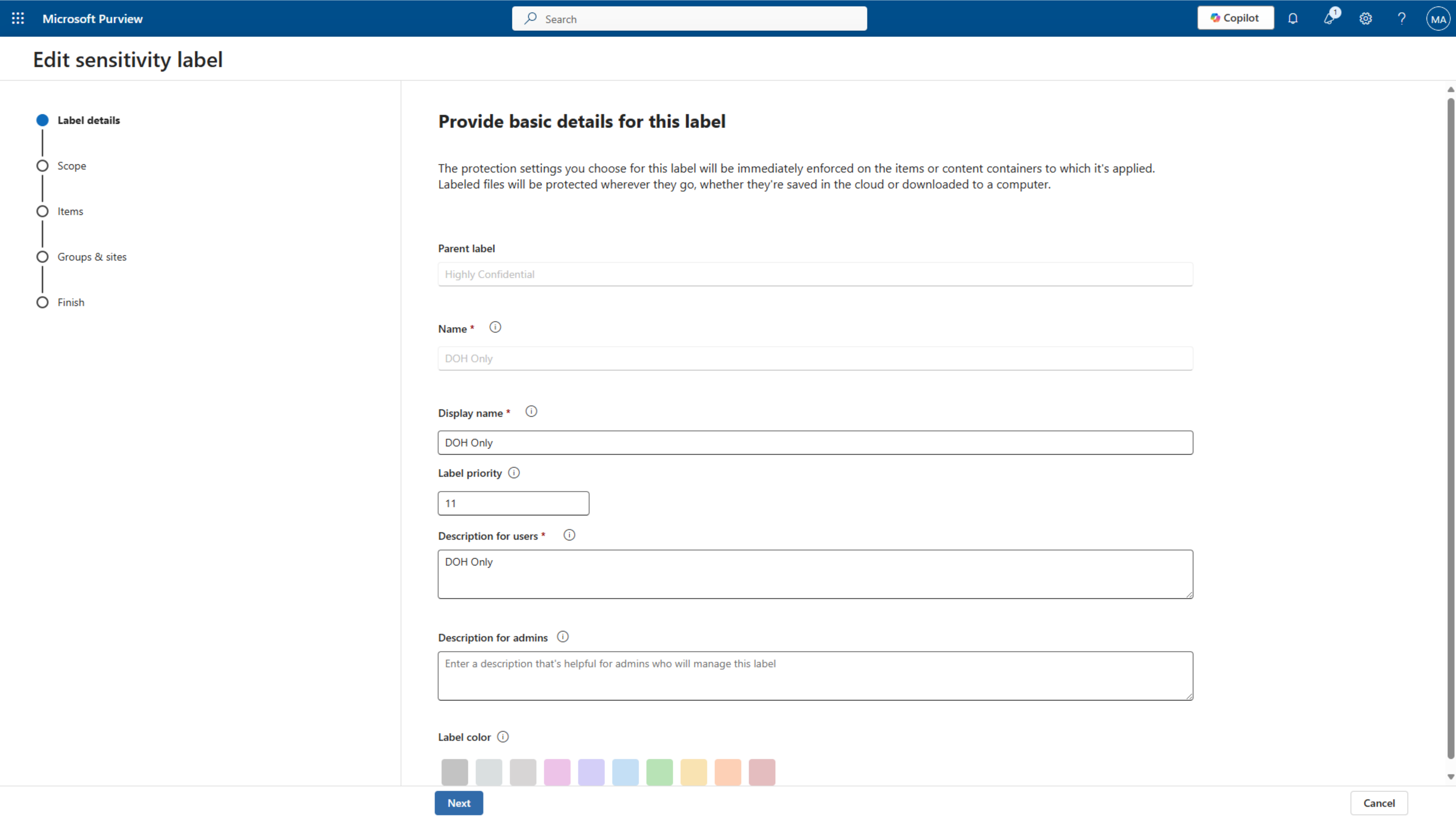


Sensitivity labels

ⓘ You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

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	Priority	Scope	Created by	Last modified
Personal	0	File, Email		Oct 24, 2024 6:58:29 PM
Public	1	File, Email		Oct 24, 2024 6:58:31 PM
General	2	File, Email		Oct 24, 2024 6:58:36 PM
Confidential	5	File, Email		Oct 24, 2024 6:58:43 PM
All Employees	6	File, Email		May 6, 2025 4:32:00 PM
Specific People	7	File, Email		May 6, 2025 4:32:00 PM
Highly Confidential	8	File, Email		May 6, 2025 4:32:00 PM
All Employees	9	File, Email		May 6, 2025 4:32:00 PM
Specified People	10	File, Email		May 6, 2025 4:32:00 PM
DOH Only	11	File, Email	MOD Administrator	May 6, 2025 4:41:09 PM



Edit sensitivity label

Provide basic details for this label

The protection settings you choose for this label will be immediately enforced on the items 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.

Parent label

Highly Confidential

Name *

DOH Only

Display name *

DOH Only

Label priority

11

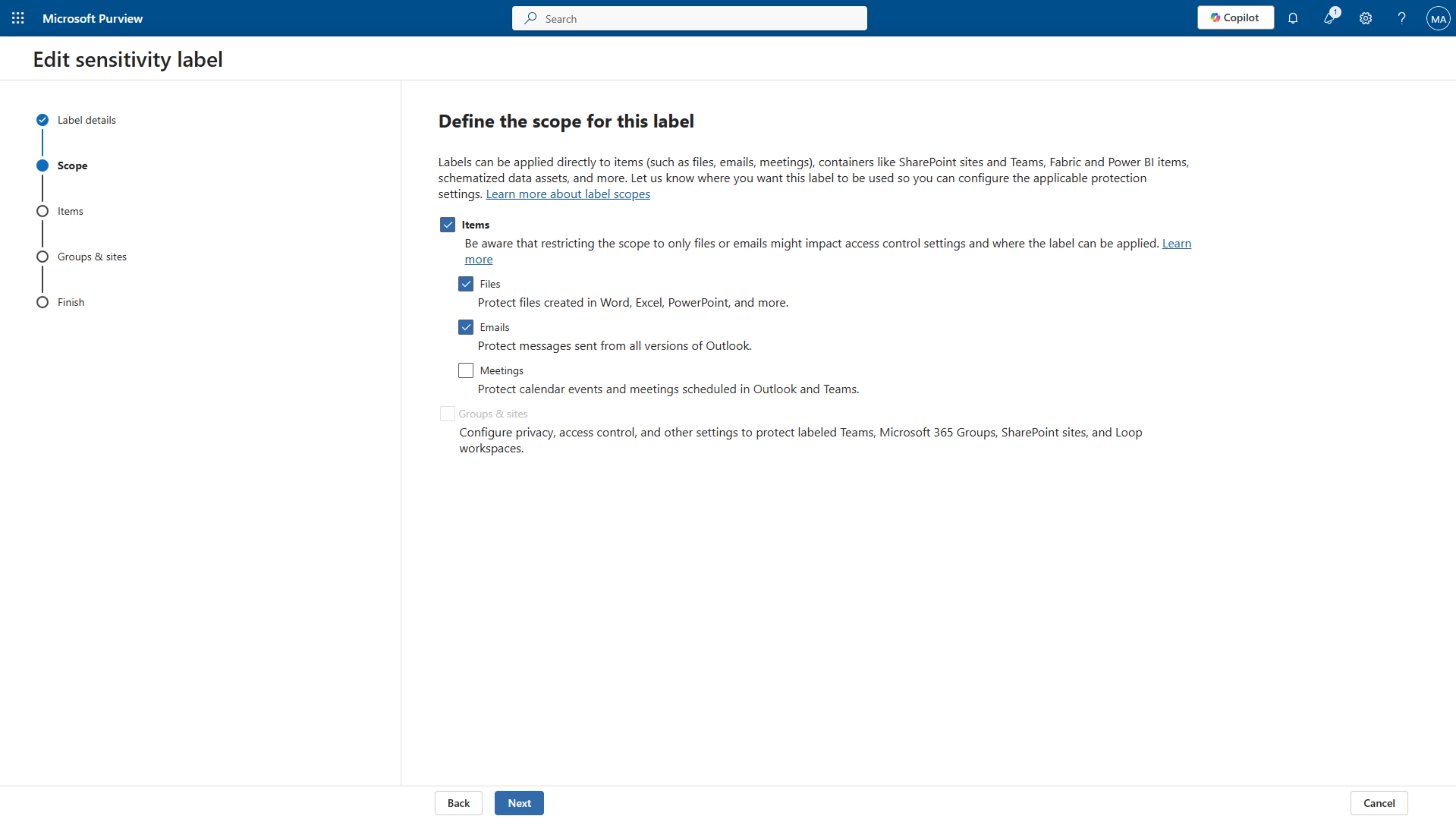
Description for users *

DOH Only

Description for admins

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

Label color



Edit sensitivity label

Define the scope for this label

Labels can be applied directly to items (such as files, emails, meetings), containers like SharePoint sites and Teams, Fabric and Power BI items, 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

☑ **Items**

Be aware that restricting the scope to only files or emails might impact access control settings and where the label can be applied. Learn more

- ☑ Files

  Protect files created in Word, Excel, PowerPoint, and more.

- ☑ Emails

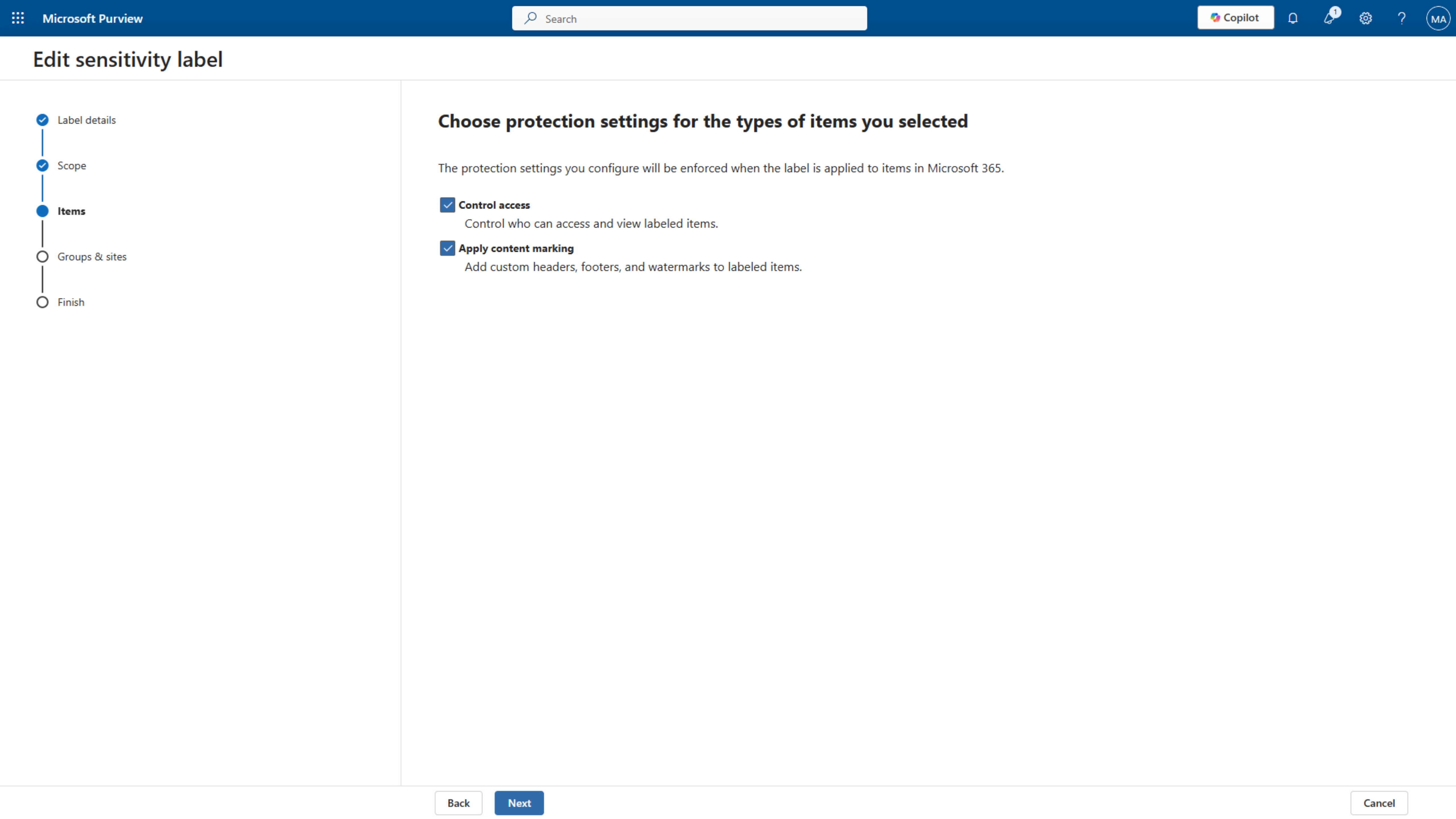
  Protect messages sent from all versions of Outlook.

- □ Meetings

  Protect calendar events and meetings scheduled in Outlook and Teams.

□ Groups & sites

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



Edit sensitivity label

Choose protection settings for the types of items you selected

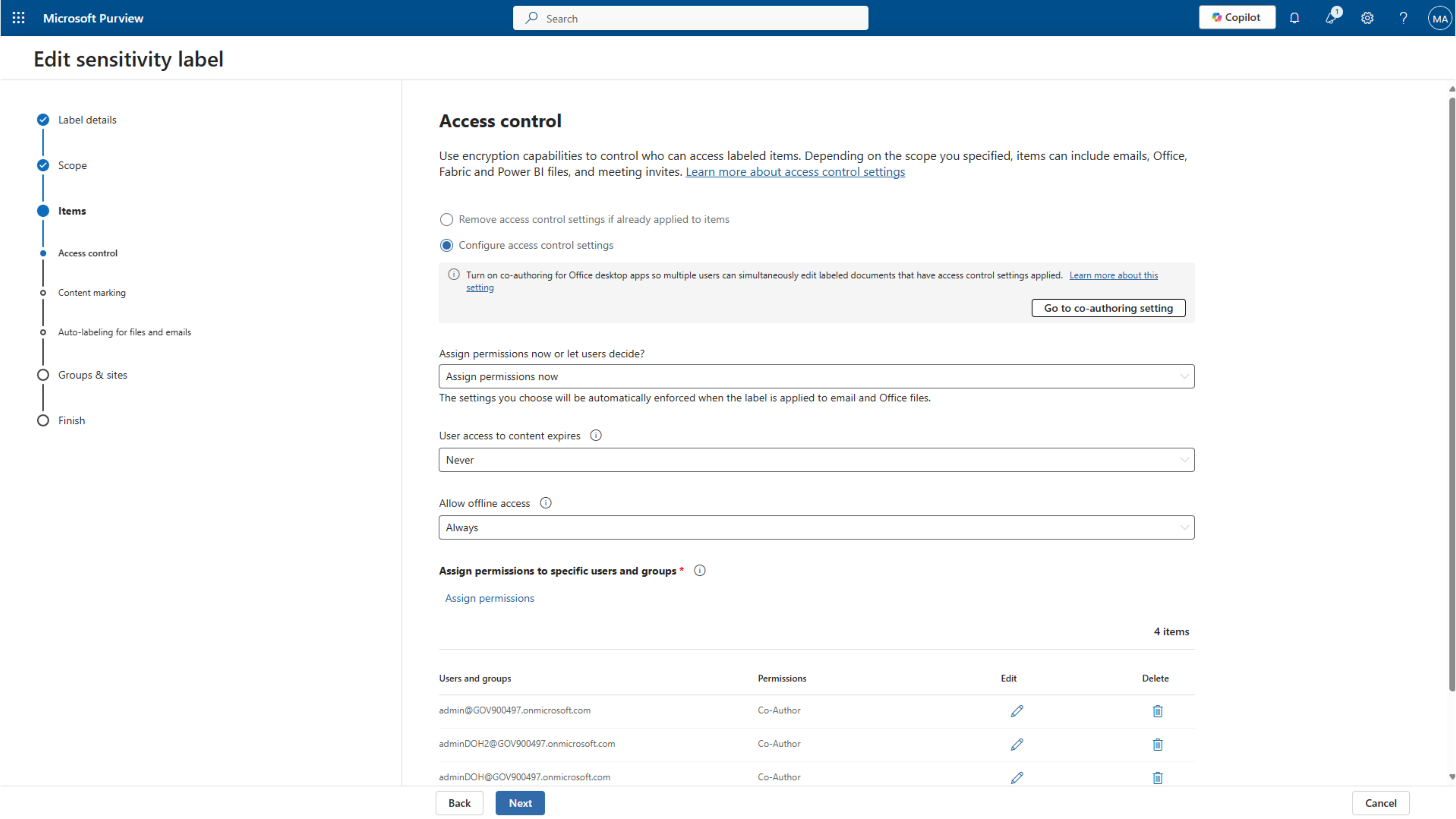
The protection settings you configure will be enforced when the label is applied to items in Microsoft 365.

☑ **Control access**

Control who can access and view labeled items.

☑ **Apply content marking**

Add custom headers, footers, and watermarks to labeled items.



Edit sensitivity label

Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. Learn more about access control settings

○ Remove access control settings if already applied to items

● Configure access control settings

ⓘ Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. Learn more about this setting

Go to co-authoring setting

Assign permissions now or let users decide?

Assign permissions now

The 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 ⓘ

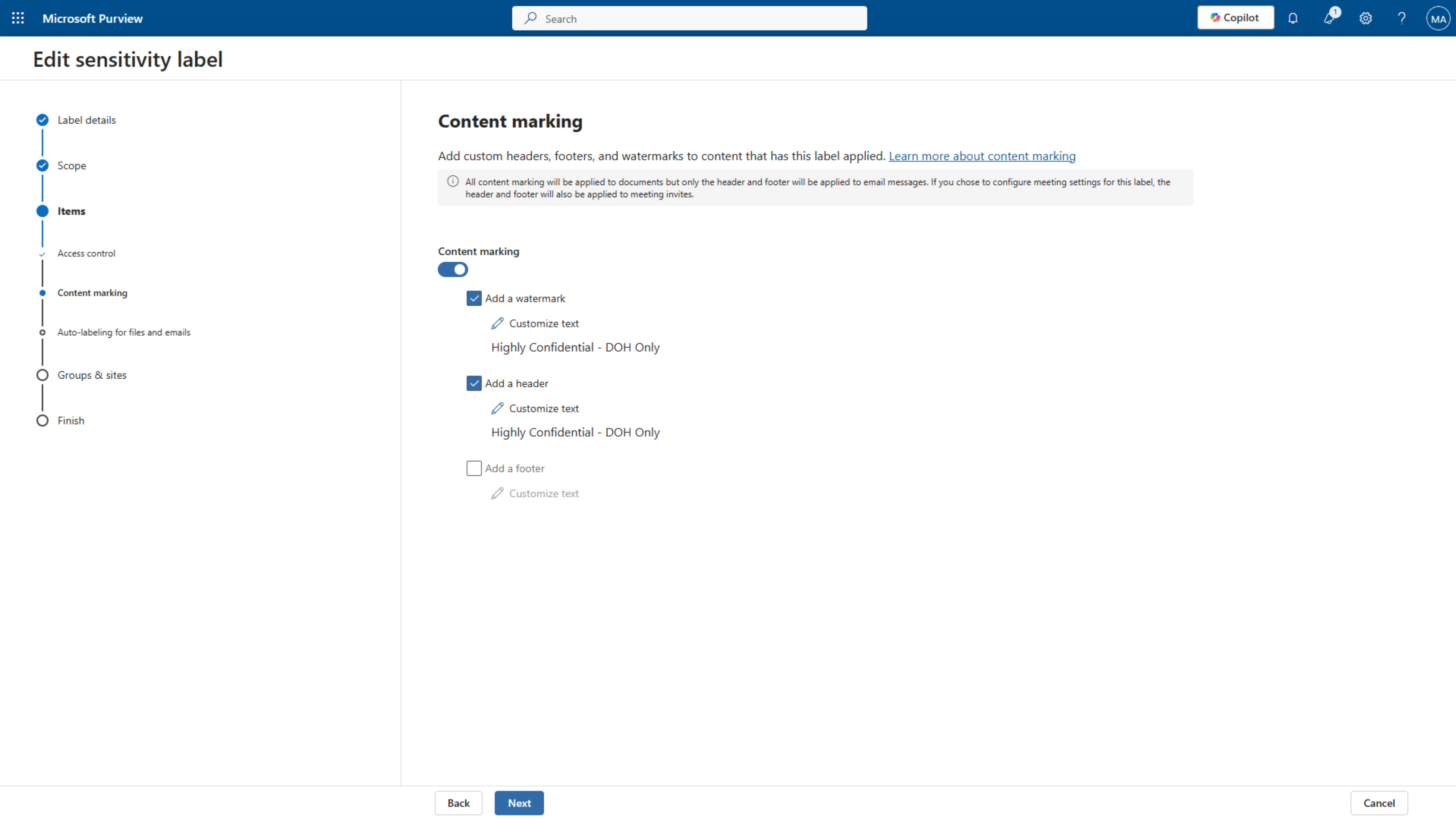
Always

Assign permissions to specific users and groups * ⓘ

Assign permissions

4 items

Users and groups	Permissions	Edit	Delete
admin@GOV900497.onmicrosoft.com	Co-Author	✎	🗑
adminDOH2@GOV900497.onmicrosoft.com	Co-Author	✎	🗑
adminDOH@GOV900497.onmicrosoft.com	Co-Author	✎	🗑



Edit sensitivity label

- ✓ Label details
- ✓ Scope
- ● **Items**
  - ✓ Access control
  - ● **Content marking**
  - ○ Auto-labeling for files and emails
- ○ Groups & sites
- ○ Finish

Content marking

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

ⓘ All content marking will be applied to documents but only the header and footer will be applied to email messages. If you chose to configure meeting settings for this label, the header and footer will also be applied to meeting invites.

Content marking

● On

☑ Add a watermark

Customize text

Highly Confidential - DOH Only

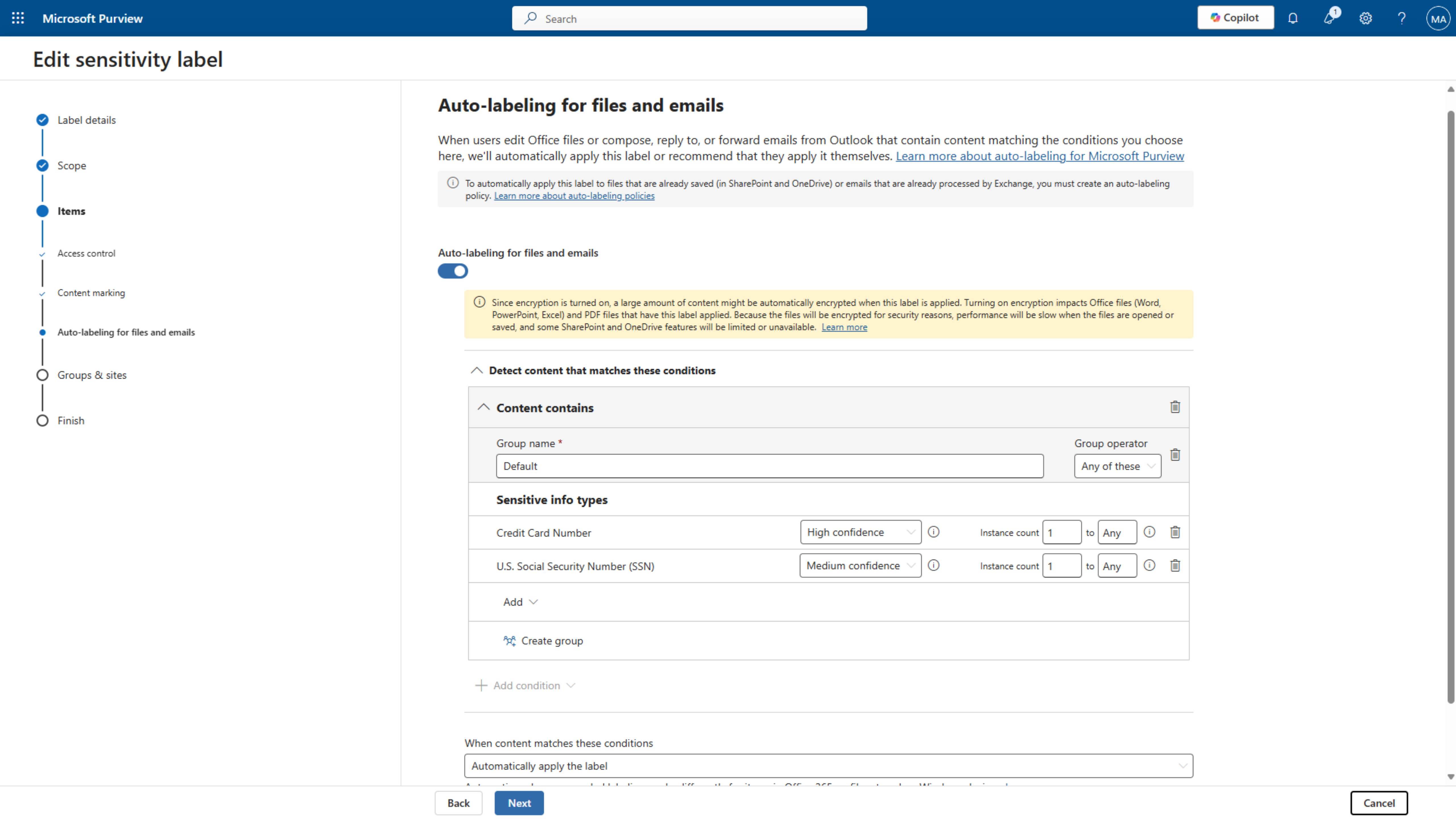
☑ Add a header

Customize text

Highly Confidential - DOH Only

□ Add a footer

Customize text



Edit 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 Purview

ⓘ 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

● On

ⓘ Since encryption is turned on, a large amount of content might be automatically encrypted when this label is applied. Turning on encryption impacts Office files (Word, PowerPoint, Excel) and PDF files 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

Detect content that matches these conditions

Content contains

Group name * Default

Group operator: Any of these

Sensitive info types

Credit Card Number	High confidence	Instance count	1	to	Any
U.S. Social Security Number (SSN)	Medium confidence	Instance count	1	to	Any

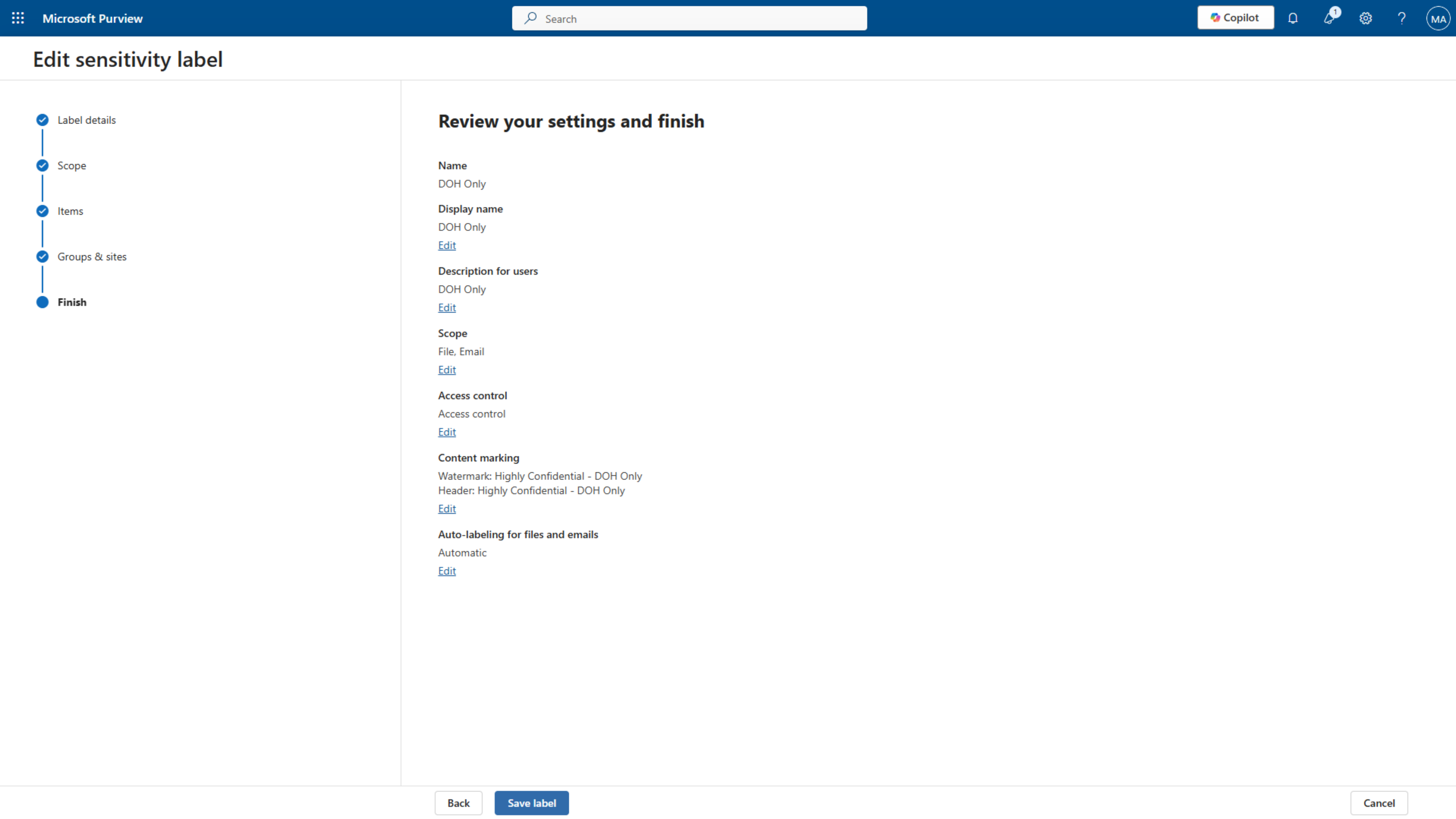
Add

Create group

+ Add condition

When content matches these conditions

Automatically apply the label



Edit sensitivity label

Review your settings and finish

Name

DOH Only

Display name

DOH Only

Edit

Description for users

DOH Only

Edit

Scope

File, Email

Edit

Access control

Access control

Edit

Content marking

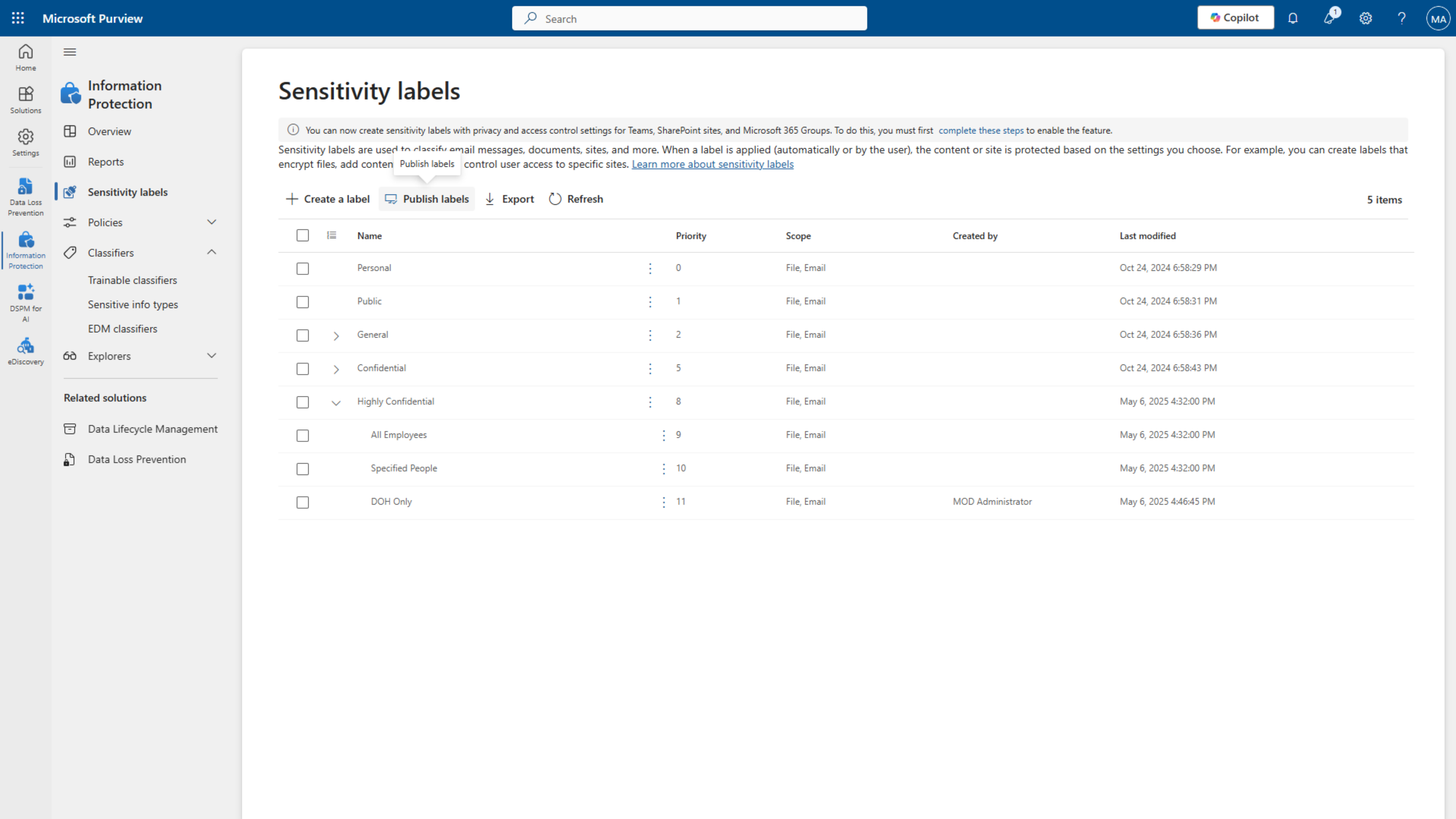
Watermark: Highly Confidential - DOH Only
Header: Highly Confidential - DOH Only

Edit

Auto-labeling for files and emails

Automatic

Edit

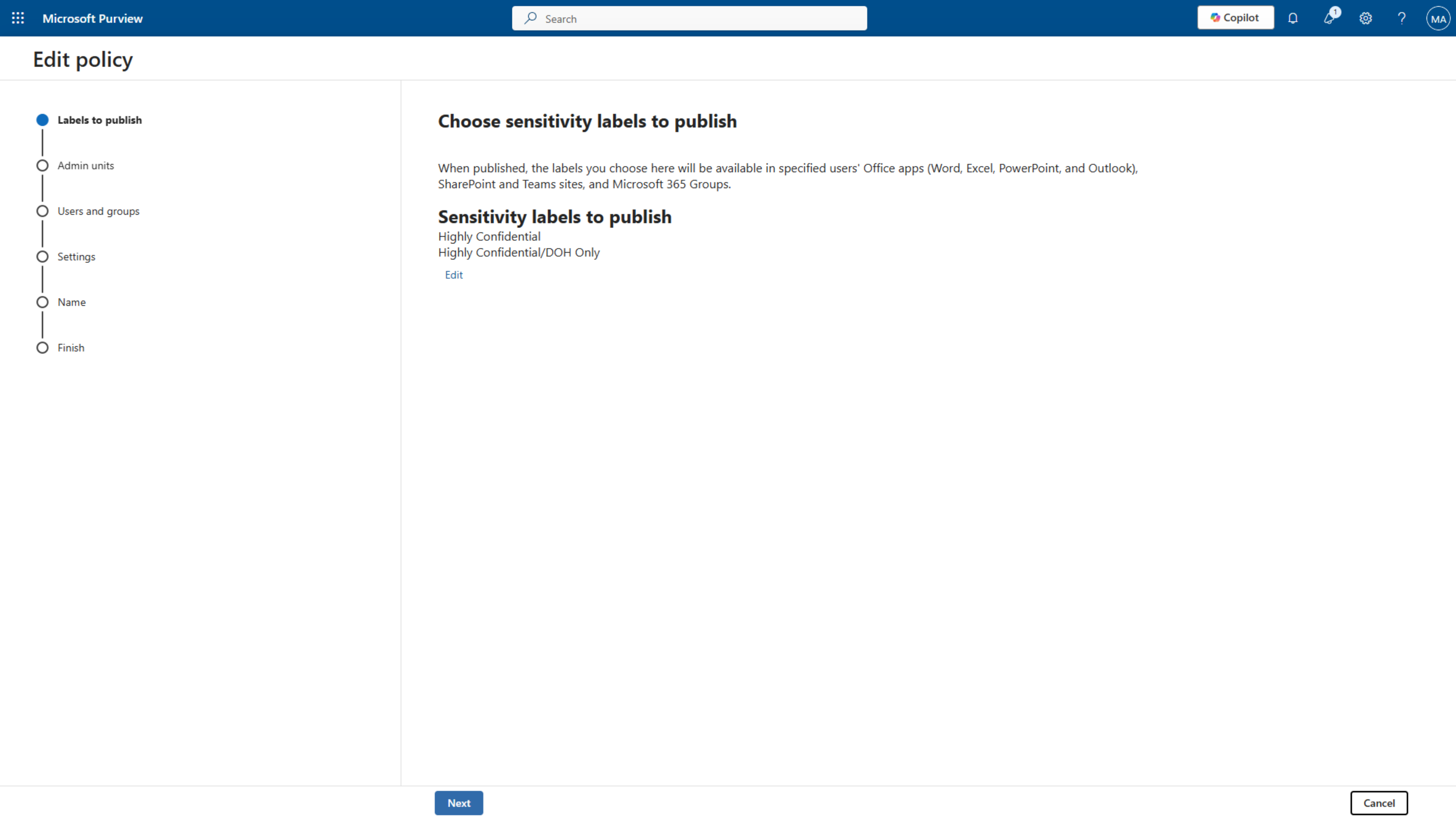


Sensitivity labels

ⓘ You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

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 conten control user access to specific sites. Learn more about sensitivity labels

Name	Priority	Scope	Created by	Last modified
Personal	0	File, Email		Oct 24, 2024 6:58:29 PM
Public	1	File, Email		Oct 24, 2024 6:58:31 PM
General	2	File, Email		Oct 24, 2024 6:58:36 PM
Confidential	5	File, Email		Oct 24, 2024 6:58:43 PM
Highly Confidential	8	File, Email		May 6, 2025 4:32:00 PM
All Employees	9	File, Email		May 6, 2025 4:32:00 PM
Specified People	10	File, Email		May 6, 2025 4:32:00 PM
DOH Only	11	File, Email	MOD Administrator	May 6, 2025 4:46:45 PM



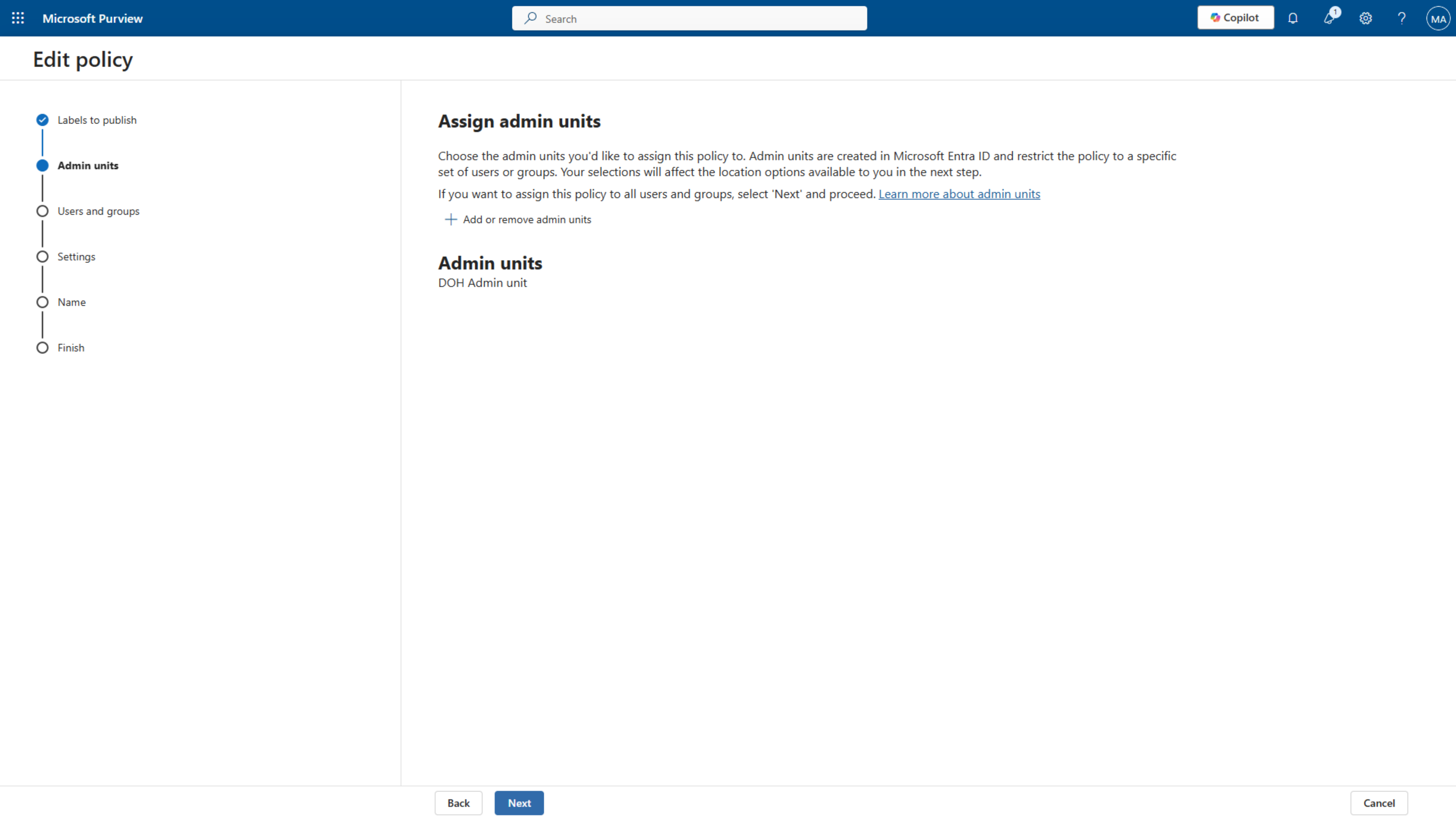
Edit policy

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

Highly Confidential
Highly Confidential/DOH Only



Edit policy

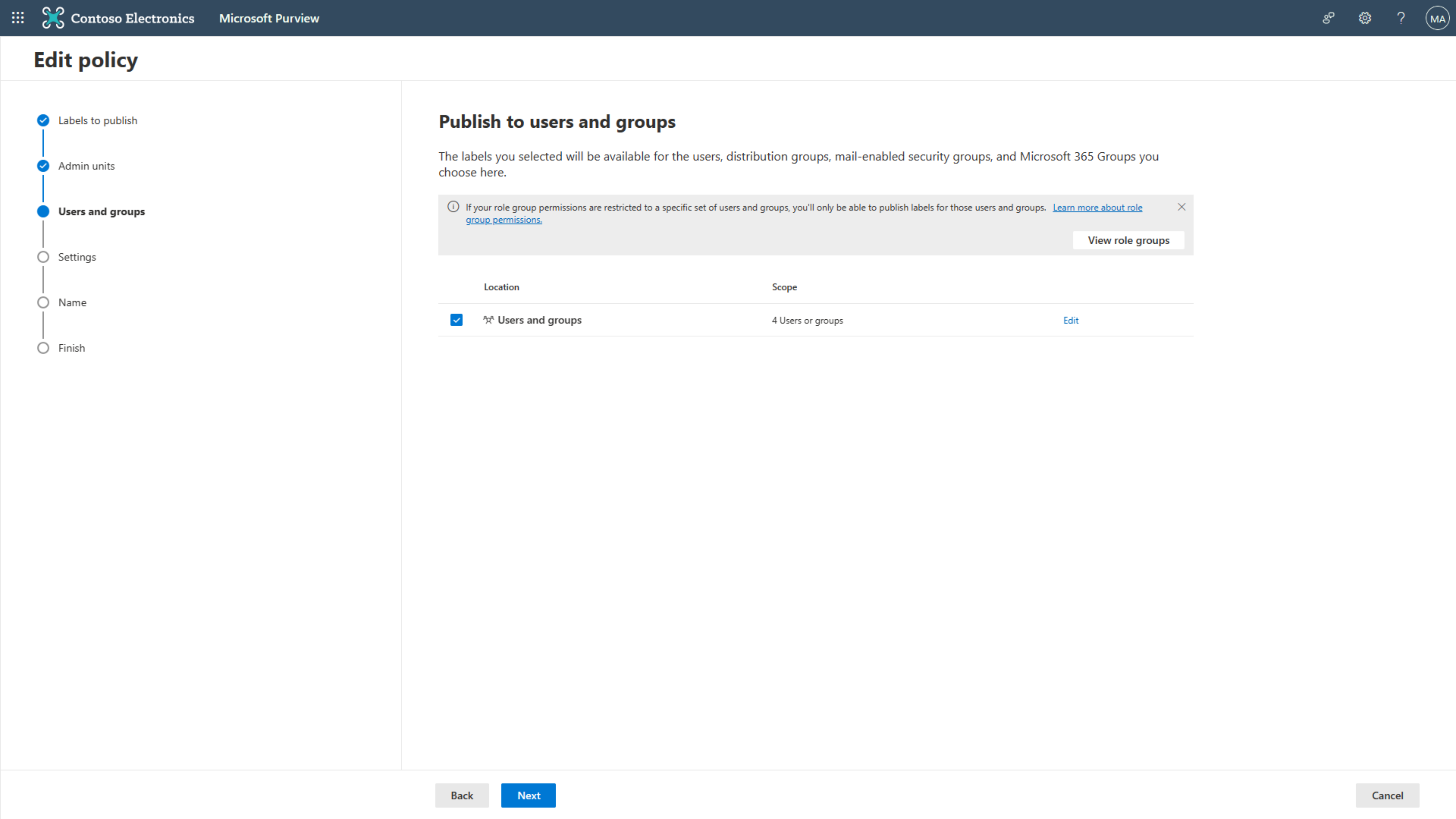
Assign admin units

Choose the admin units you'd like to assign this policy to. Admin units are created in Microsoft Entra ID and restrict the policy to a specific set of users or groups. Your selections will affect the location options available to you in the next step.

If you want to assign this policy to all users and groups, select 'Next' and proceed. Learn more about admin units

Admin units

DOH Admin unit



Edit policy

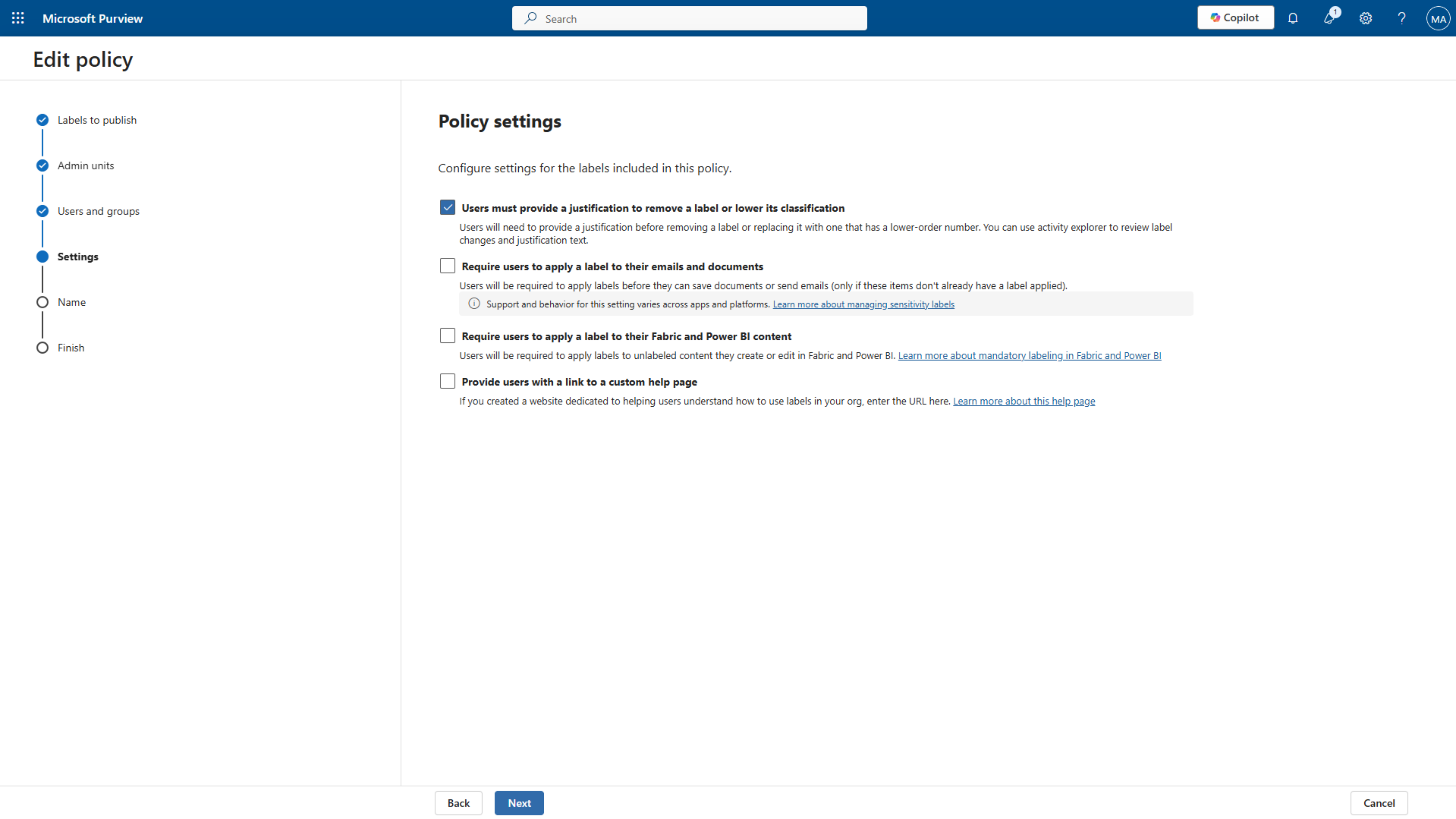
- ✓ Labels to publish
- ✓ Admin units
- ● **Users and groups**
- ○ Settings
- ○ Name
- ○ Finish

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.

ⓘ If your role group permissions are restricted to a specific set of users and groups, you'll only be able to publish labels for those users and groups. Learn more about role group permissions.

	Location	Scope	
☑	Users and groups	4 Users or groups	Edit



Edit policy

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

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 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 or send emails (only if these items don't already have a label applied).

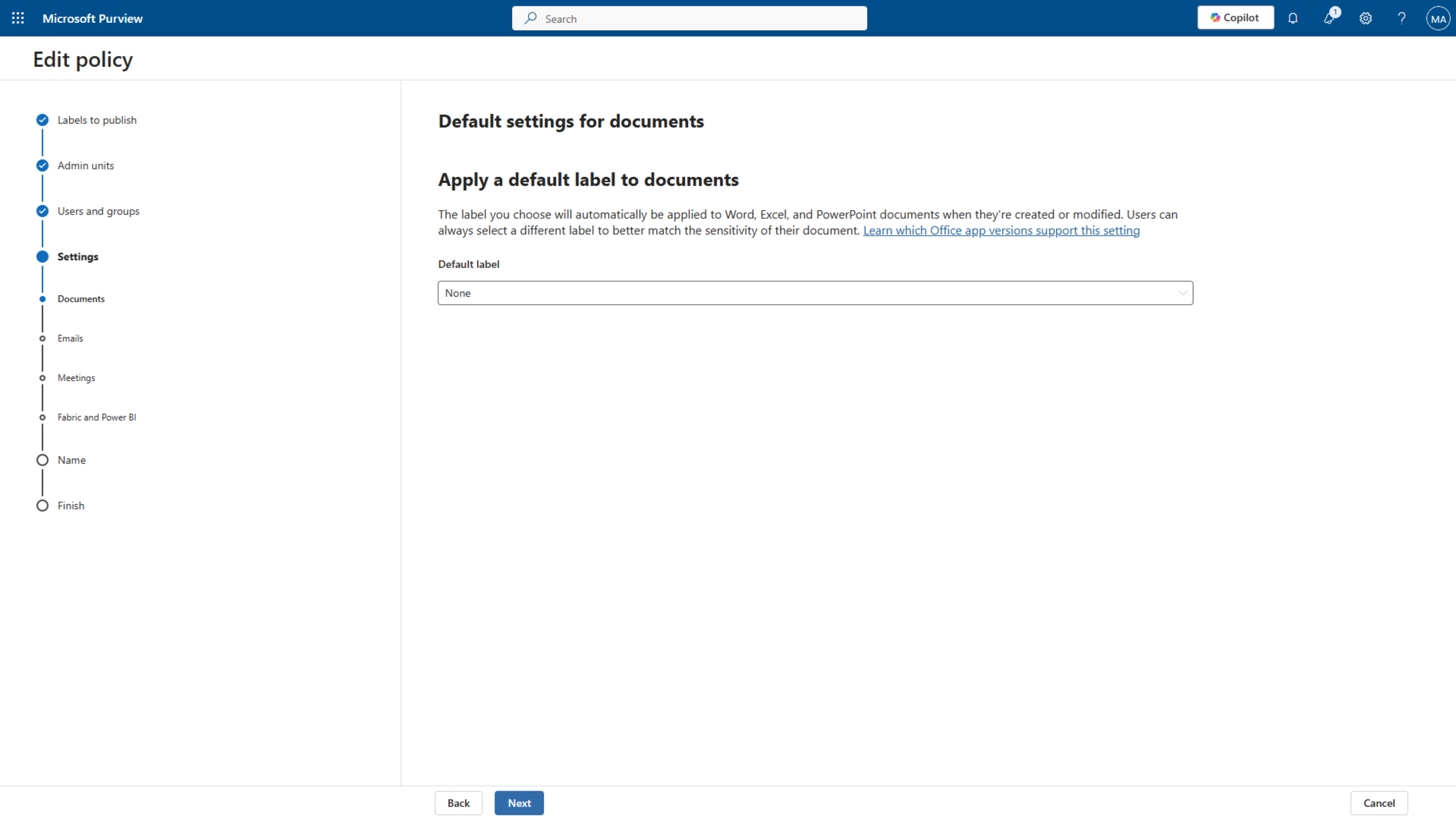
ⓘ Support and behavior for this setting varies across apps and platforms. Learn more about managing sensitivity labels

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

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



Edit policy

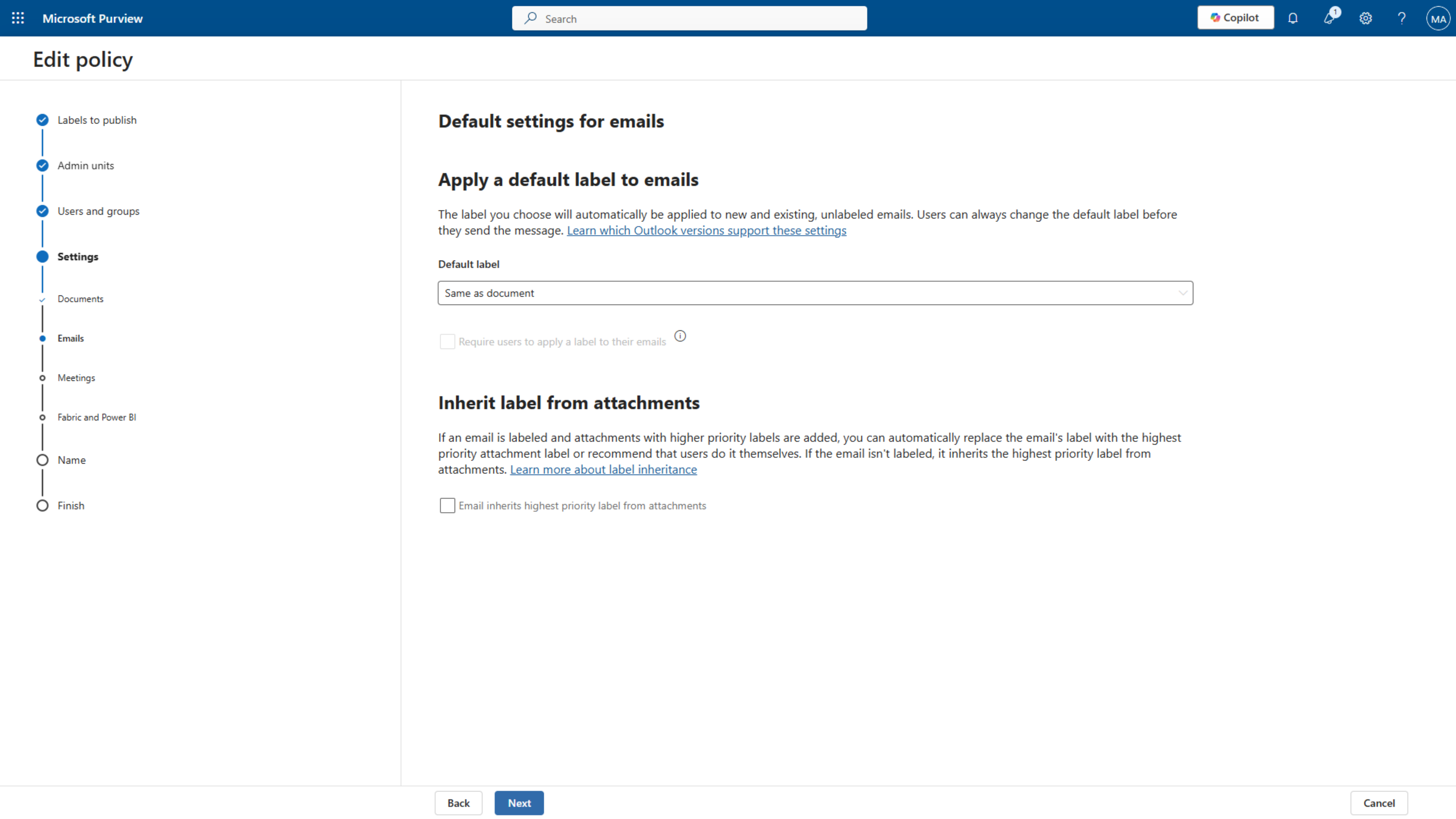
Default settings for documents

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. Learn which Office app versions support this setting

Default label

None



Edit policy

Default settings for emails

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. Learn which Outlook versions support these settings

Default label

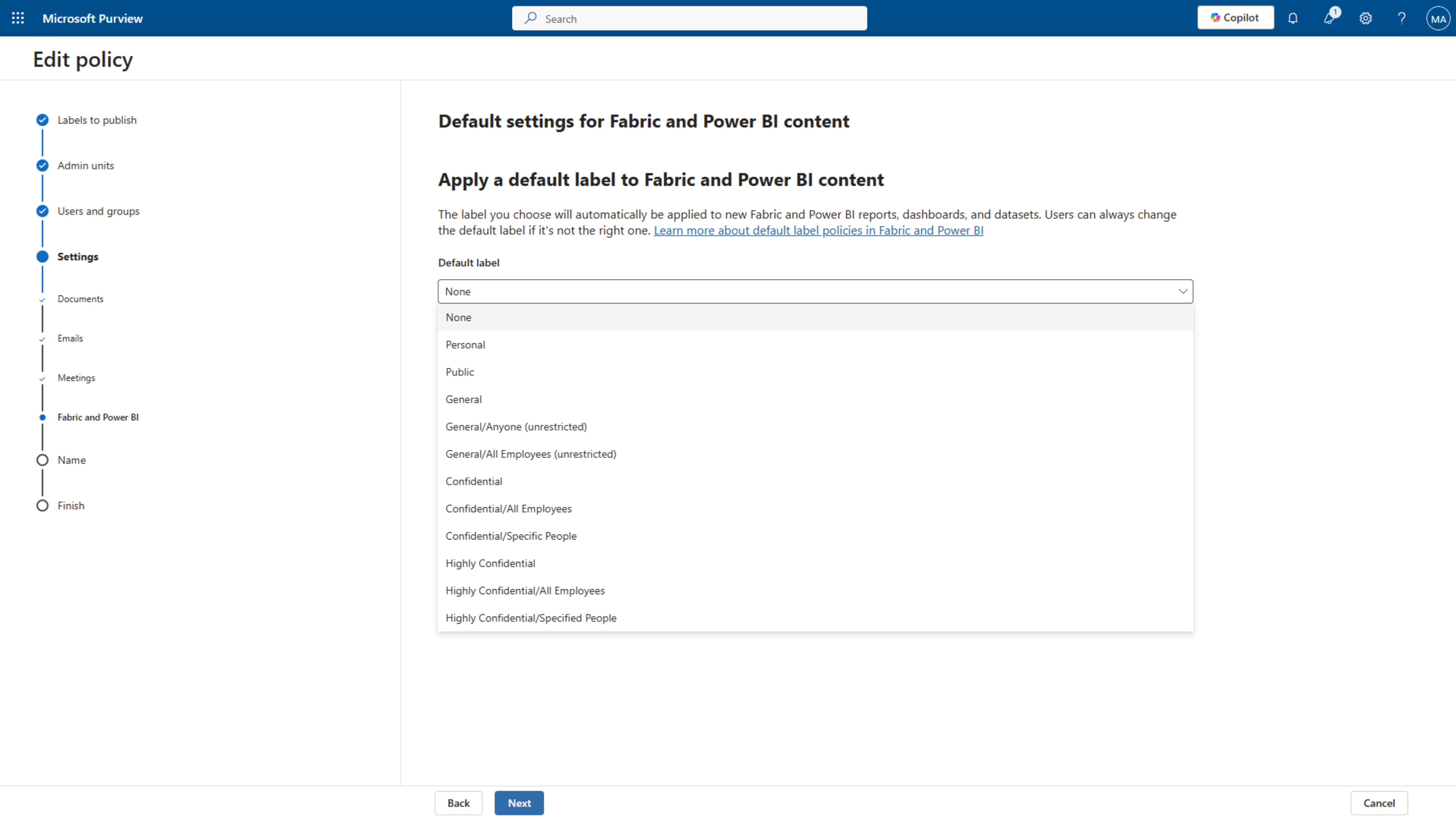
Same as document

□ Require users to apply a label to their emails

Inherit label from attachments

If an email is labeled and attachments with higher priority labels are added, you can automatically replace the email's label with the highest priority attachment label or recommend that users do it themselves. If the email isn't labeled, it inherits the highest priority label from attachments. Learn more about label inheritance

□ Email inherits highest priority label from attachments



Edit policy

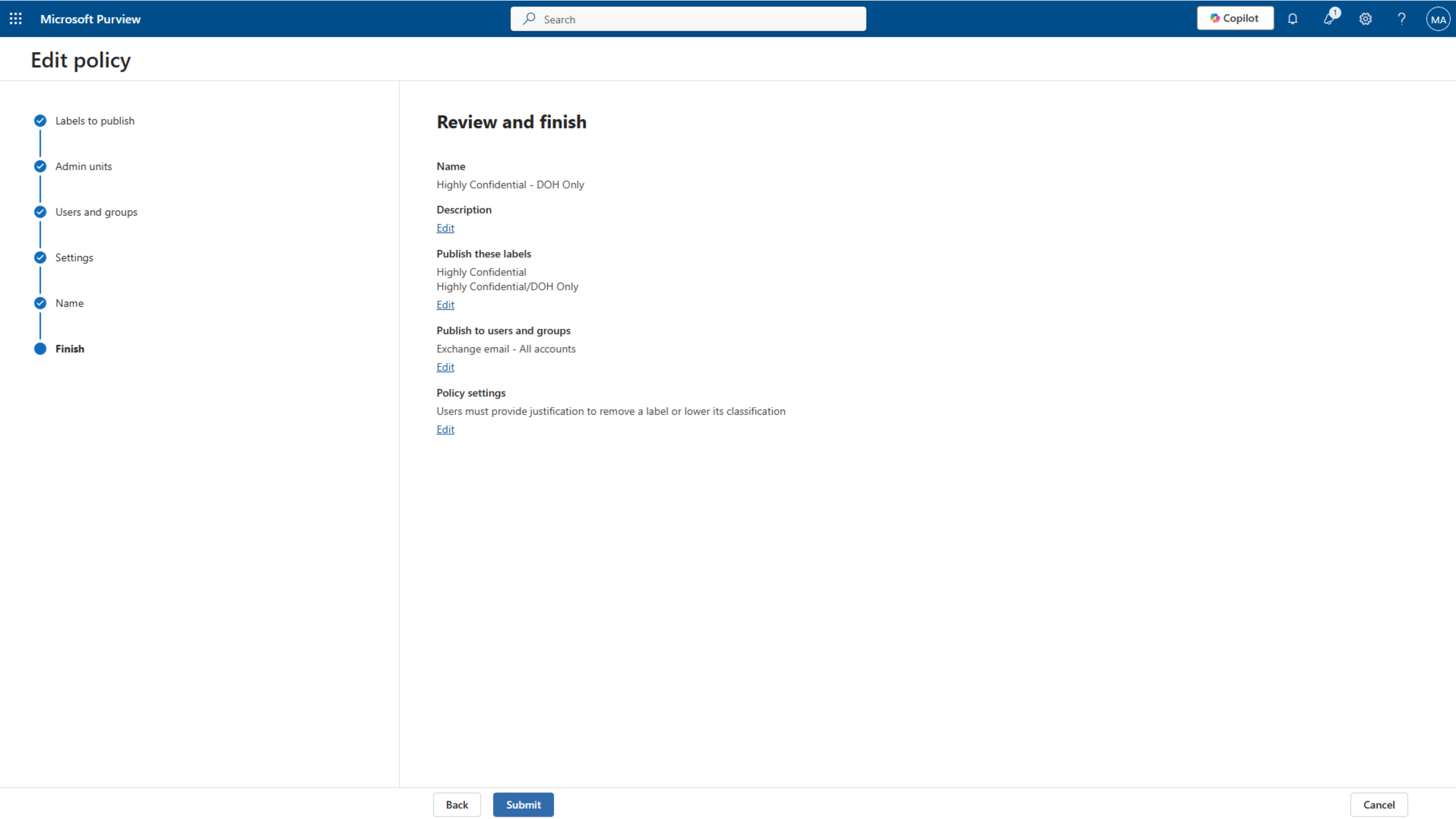
Default settings for Fabric and Power BI content

Apply a default label to Fabric and Power BI content

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

Default label

None



Edit policy

Review and finish

Name

Highly Confidential - DOH Only

Description

Edit

Publish these labels

Highly Confidential
Highly Confidential/DOH Only

Edit

Publish to users and groups

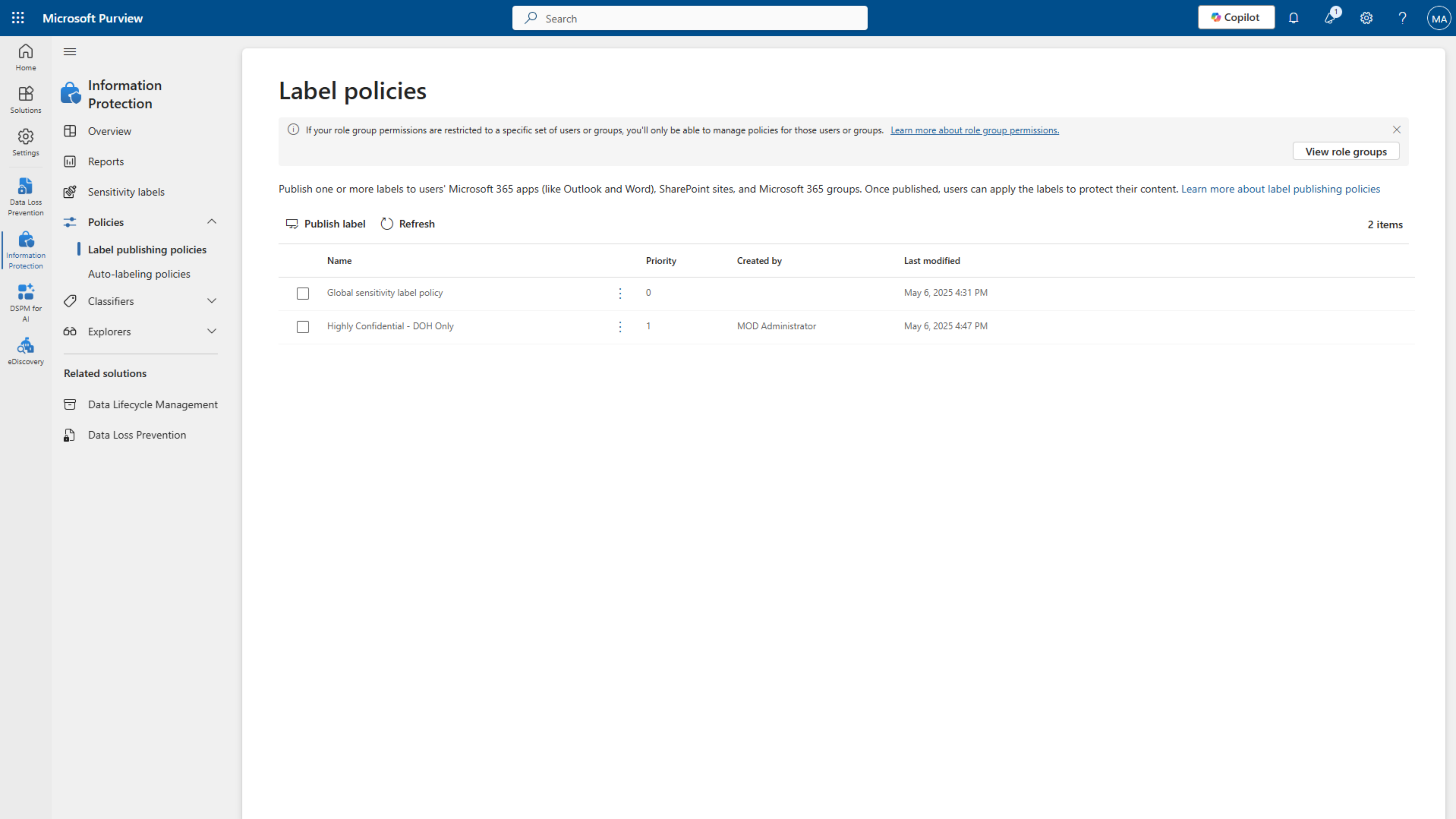
Exchange email - All accounts

Edit

Policy settings

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

Edit



Label policies

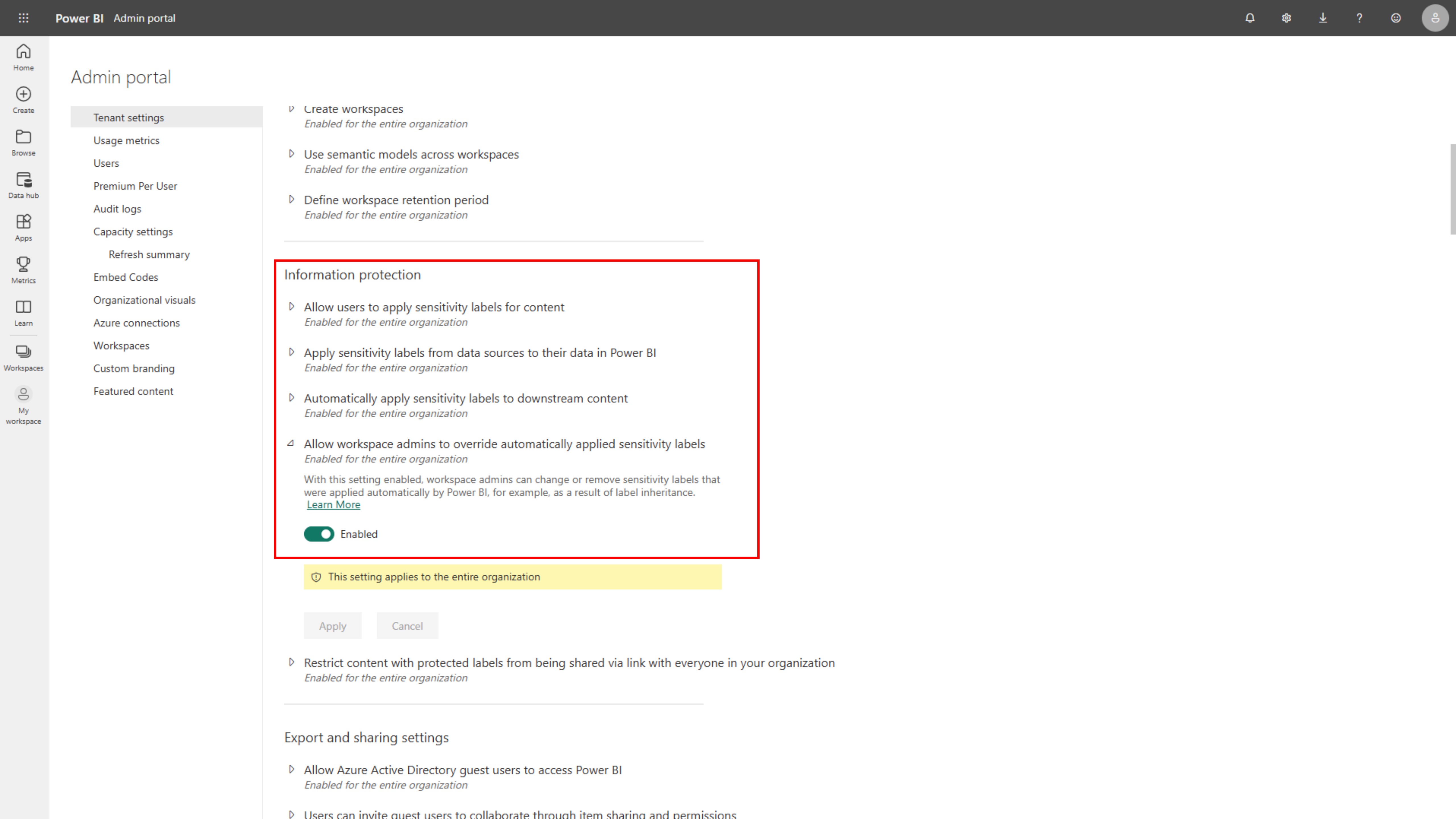
If your role group permissions are restricted to a specific set of users or groups, you'll only be able to manage policies for those users or groups. Learn more about role group permissions.

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

2 items

	Name	Priority	Created by	Last modified
□	Global sensitivity label policy	0		May 6, 2025 4:31 PM
□	Highly Confidential - DOH Only	1	MOD Administrator	May 6, 2025 4:47 PM

Enable Sensitivity labeling in Power BI Admin center



Create workspaces
Enabled for the entire organization

Use semantic models across workspaces
Enabled for the entire organization

Define workspace retention period
Enabled 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

With this setting enabled, workspace admins can change or remove sensitivity labels that were applied automatically by Power BI, for example, as a result of label inheritance. Learn More

● Enabled

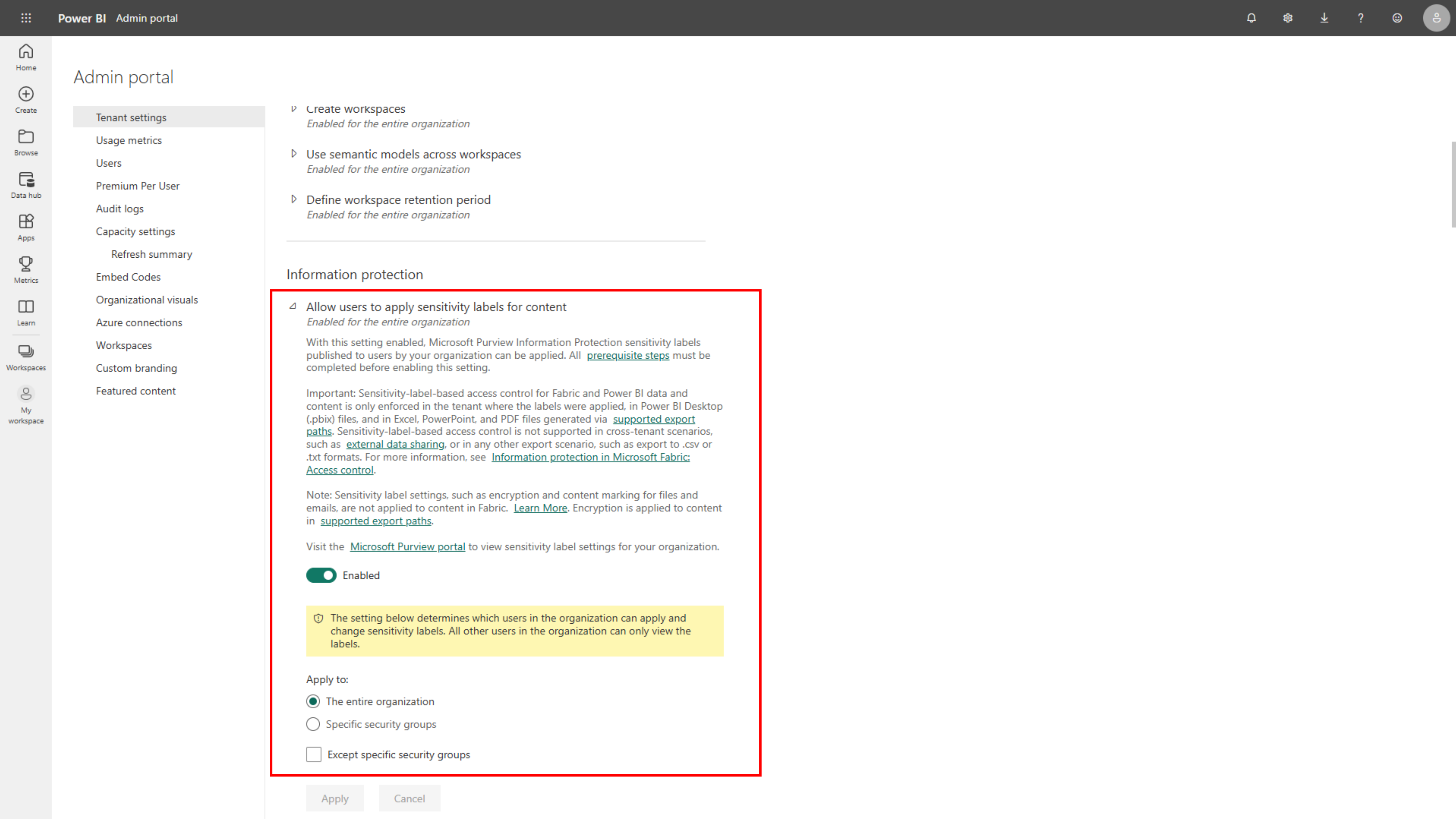
This setting applies to the entire organization

Restrict content with protected labels from being shared via link with everyone in your organization
Enabled for the entire organization

Export and sharing settings

Allow Azure Active Directory guest users to access Power BI
Enabled for the entire organization

Users can invite guest users to collaborate through item sharing and permissions



Admin portal

▹ Create workspaces
Enabled for the entire organization

▹ Use semantic models across workspaces
Enabled for the entire organization

▹ Define workspace retention period
Enabled for the entire organization

Information protection

◢ Allow users to apply sensitivity labels for content
Enabled for the entire organization

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.

Important: Sensitivity-label-based access control for Fabric and Power BI data and content is only enforced in the tenant where the labels were applied, in Power BI Desktop (.pbix) files, and in Excel, PowerPoint, and PDF files generated via supported export paths. Sensitivity-label-based access control is not supported in cross-tenant scenarios, such as external data sharing, or in any other export scenario, such as export to .csv or .txt formats. For more information, see Information protection in Microsoft Fabric: Access control.

Note: Sensitivity label settings, such as encryption and content marking for files and emails, are not applied to content in Fabric. Learn More. Encryption is applied to content in supported export paths.

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

Enabled

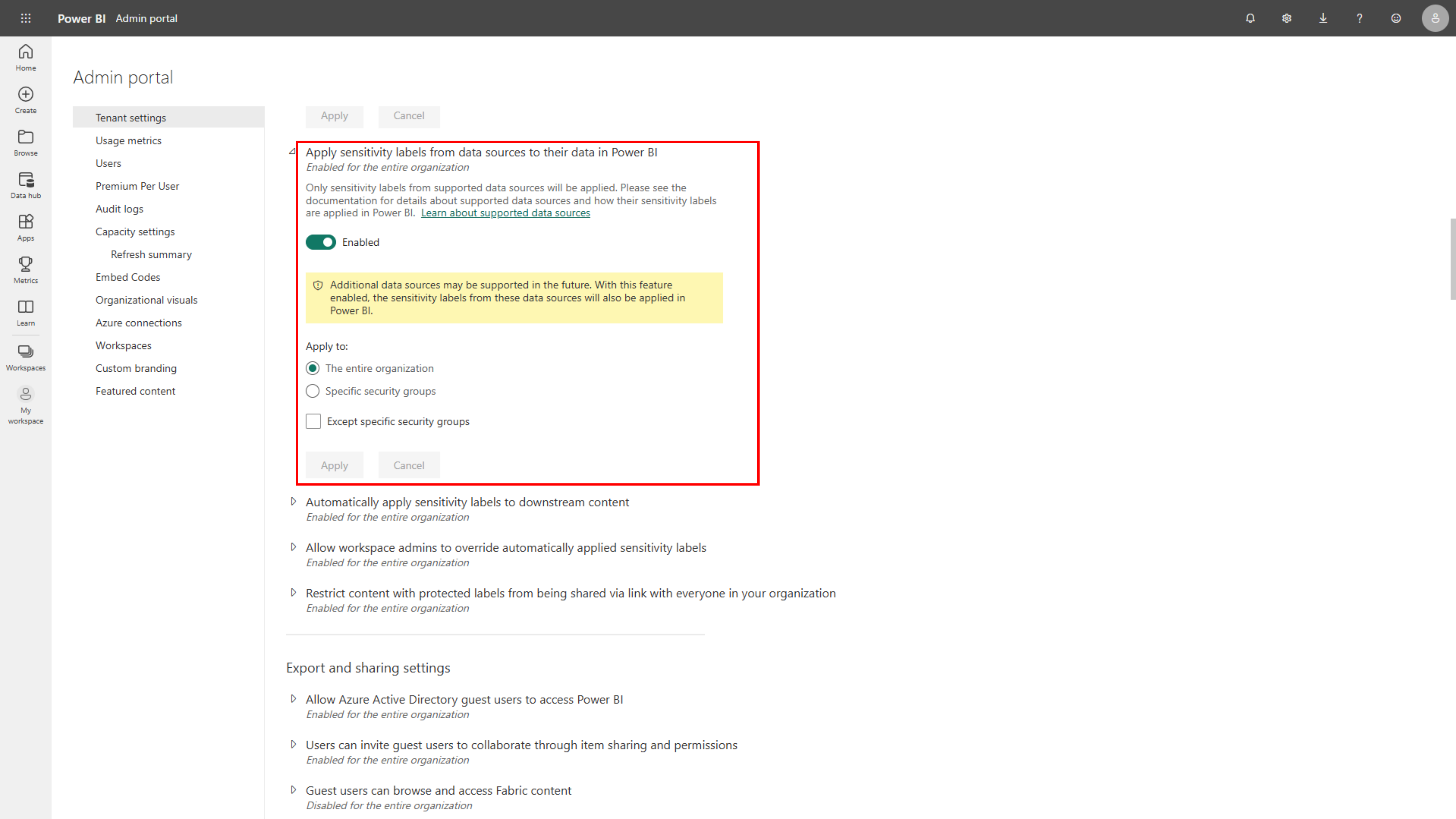
The setting below determines which users in the organization can apply and change sensitivity labels. All other users in the organization can only view the labels.

Apply to:

● The entire organization

○ Specific security groups

□ Except specific security groups



Admin portal

Apply sensitivity labels from data sources to their data in Power BI

Enabled for the entire organization

Only sensitivity labels from supported data sources will be applied. Please see the documentation for details about supported data sources and how their sensitivity labels are applied in Power BI. Learn about supported data sources

Enabled

Additional data sources may be supported in the future. With this feature enabled, the sensitivity labels from these data sources will also be applied in Power BI.

Apply to:

● The entire organization

○ Specific security groups

□ Except specific security groups

Apply Cancel

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

Enabled for the entire organization

Export and sharing settings

Allow Azure Active Directory guest users to access Power BI

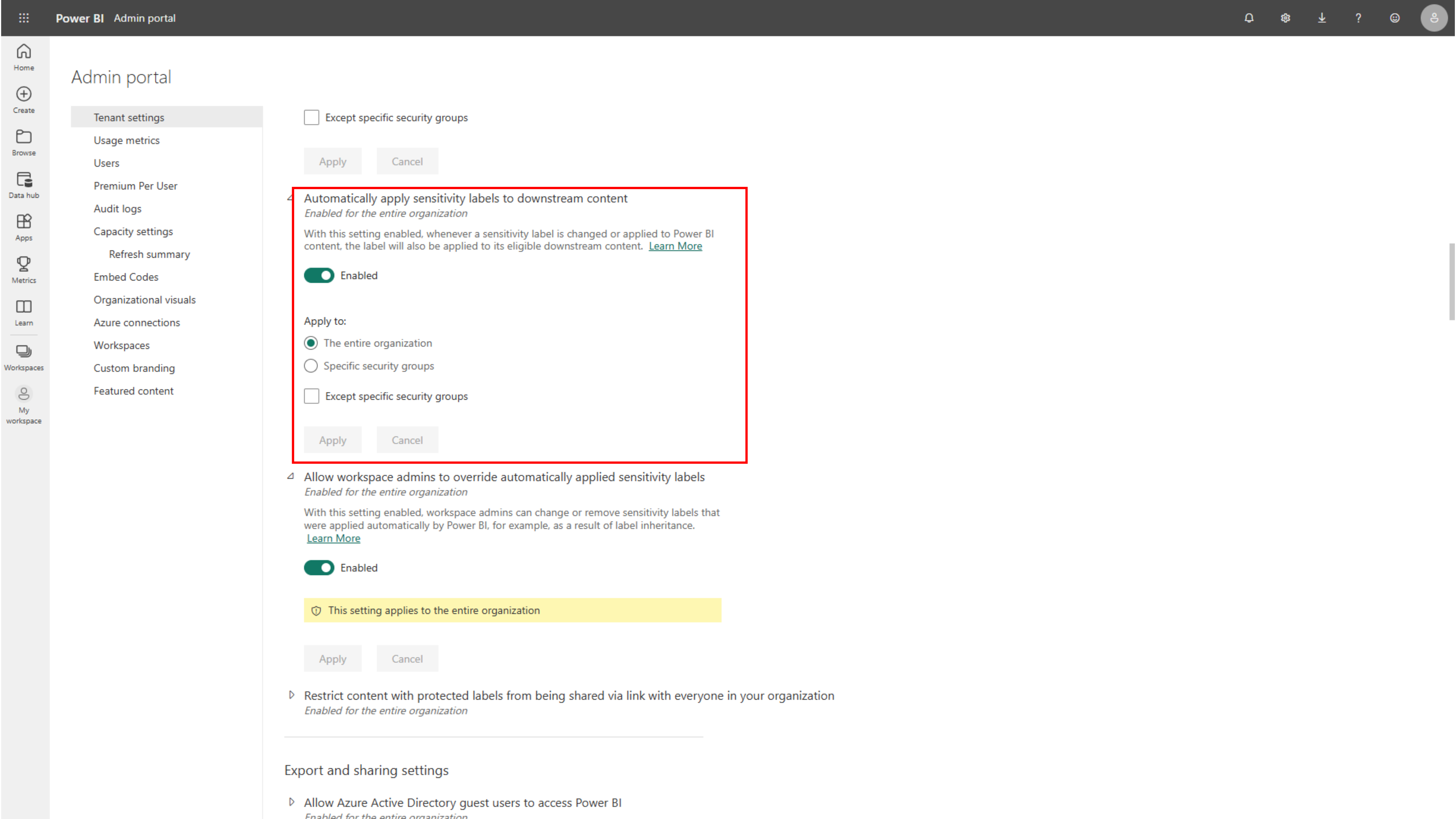
Enabled for the entire organization

Users can invite guest users to collaborate through item sharing and permissions

Enabled for the entire organization

Guest users can browse and access Fabric content

Disabled for the entire organization



Admin portal

□ Except specific security groups

Automatically apply sensitivity labels to downstream content

Enabled for the entire organization

With this setting enabled, whenever a sensitivity label is changed or applied to Power BI content, the label will also be applied to its eligible downstream content. Learn More

Enabled

Apply to:

● The entire organization

○ Specific security groups

□ Except specific security groups

Allow workspace admins to override automatically applied sensitivity labels

Enabled for the entire organization

With this setting enabled, workspace admins can change or remove sensitivity labels that were applied automatically by Power BI, for example, as a result of label inheritance. Learn More

Enabled

This setting applies to the entire organization

Restrict content with protected labels from being shared via link with everyone in your organization

Enabled for the entire organization

Export and sharing settings

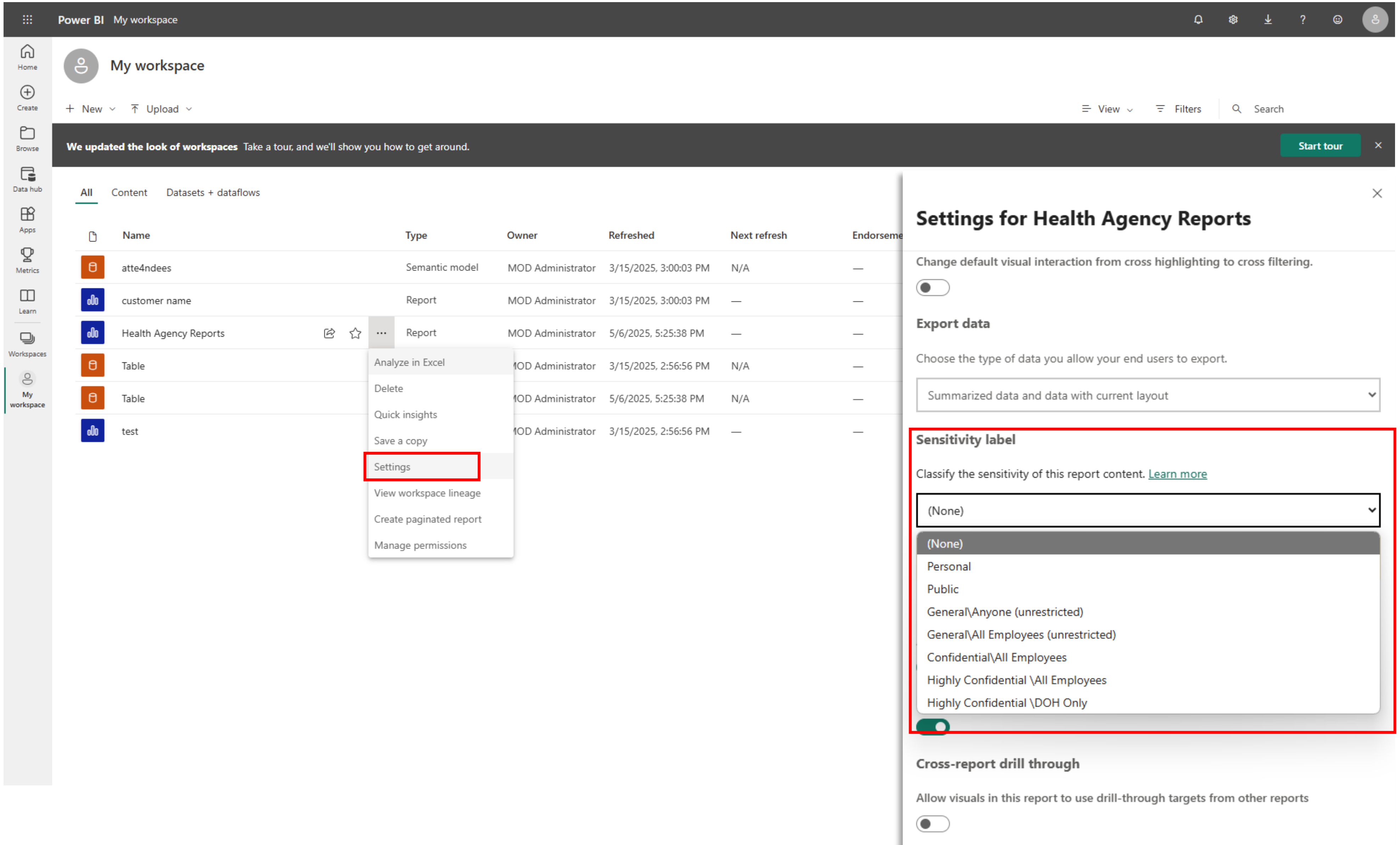
Allow Azure Active Directory guest users to access Power BI

Enabled for the entire organization

Sensitivity labeling End User experience

Sensitivity labels in the Power BI Service

Set the sensitivity label on a report or dashboard



My workspace

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

Name	Type	Owner	Refreshed	Next refresh	Endorseme
atte4ndees	Semantic model	MOD Administrator	3/15/2025, 3:00:03 PM	N/A	—
customer name	Report	MOD Administrator	3/15/2025, 3:00:03 PM	—	—
Health Agency Reports	Report	MOD Administrator	5/6/2025, 5:25:38 PM	—	—
Table		OD Administrator	3/15/2025, 2:56:56 PM	N/A	—
Table		OD Administrator	5/6/2025, 5:25:38 PM	N/A	—
test		OD Administrator	3/15/2025, 2:56:56 PM	—	—

Settings for Health Agency Reports

Change default visual interaction from cross highlighting to cross filtering.

Export data

Choose the type of data you allow your end users to export.

Summarized data and data with current layout

Sensitivity label

Classify the sensitivity of this report content. Learn more

(None)

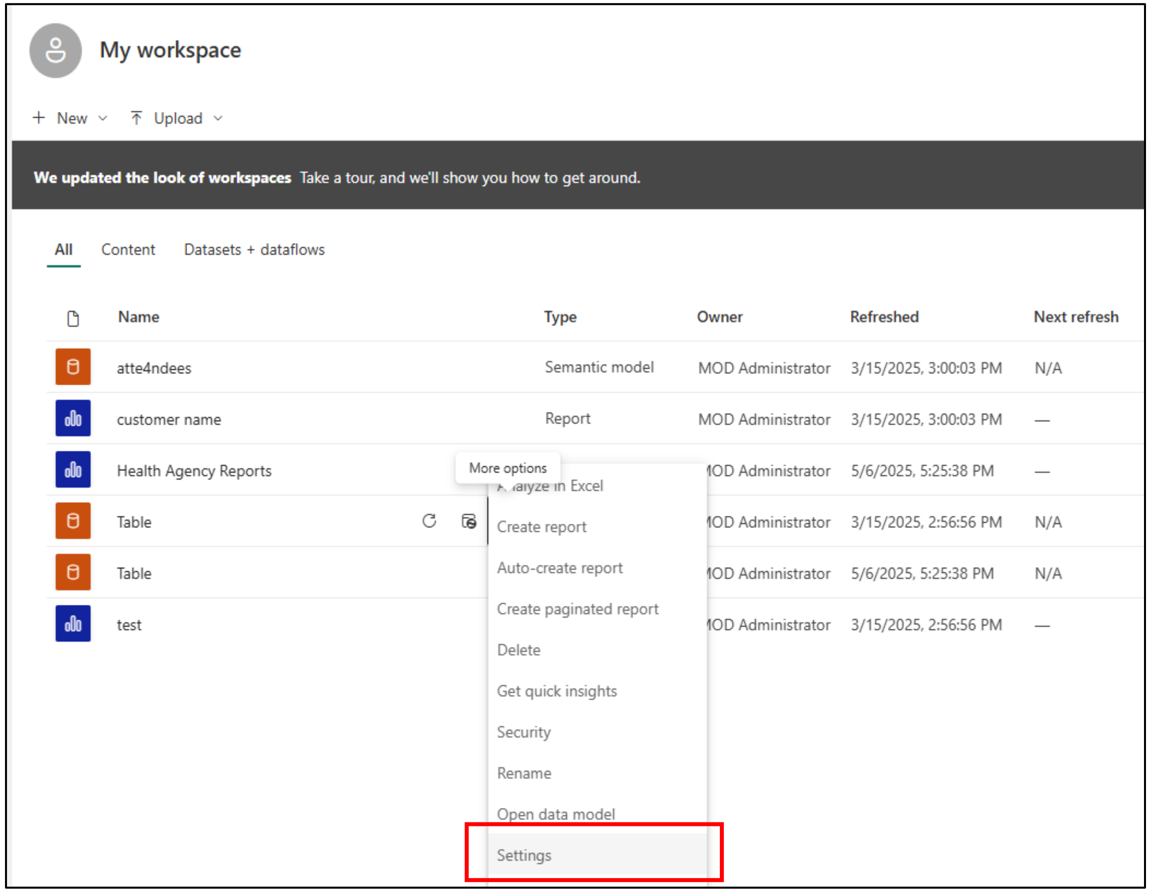
- (None)
- Personal
- Public
- General\Anyone (unrestricted)
- General\All Employees (unrestricted)
- Confidential\All Employees
- Highly Confidential \All Employees
- Highly Confidential \DOH Only

Cross-report drill through

Allow visuals in this report to use drill-through targets from other reports

Sensitivity labels in the Power BI Service

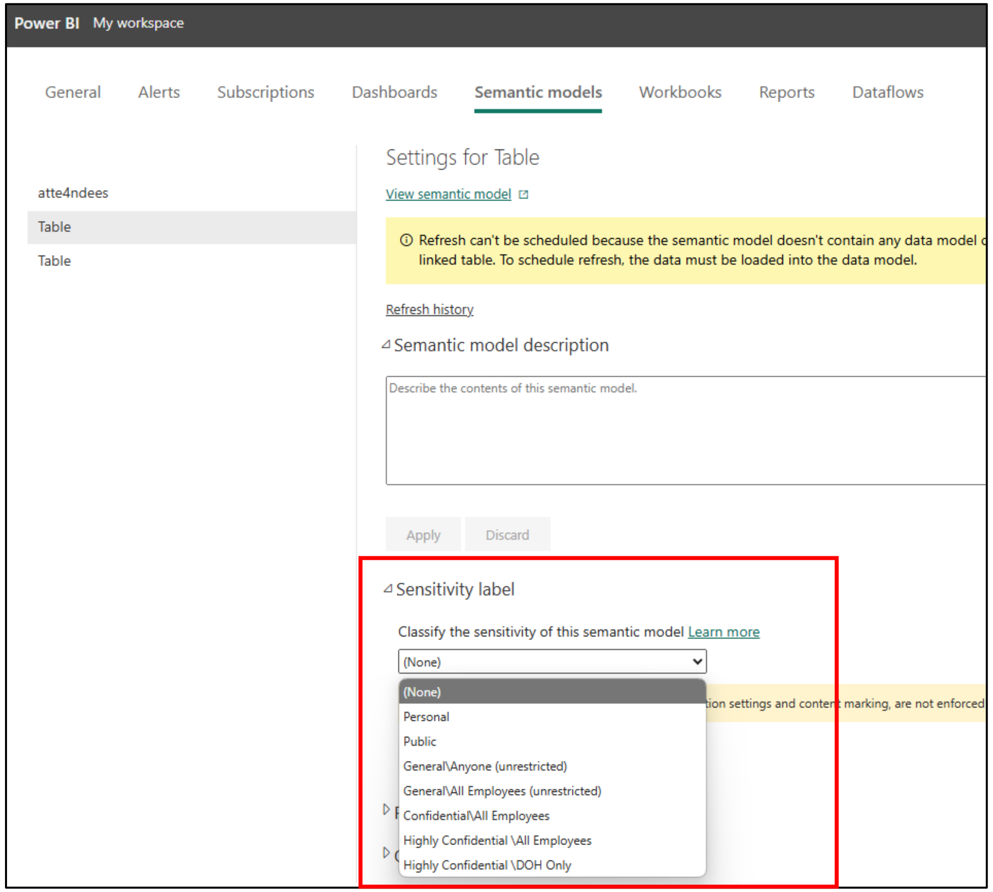
Set the sensitivity label on a semantic model or dataflow



My workspace

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

Name	Type	Owner	Refreshed	Next refresh
atte4ndees	Semantic model	MOD Administrator	3/15/2025, 3:00:03 PM	N/A
customer name	Report	MOD Administrator	3/15/2025, 3:00:03 PM	—
Health Agency Reports		IOD Administrator	5/6/2025, 5:25:38 PM	—
Table		IOD Administrator	3/15/2025, 2:56:56 PM	N/A
Table		IOD Administrator	5/6/2025, 5:25:38 PM	N/A
test		IOD Administrator	3/15/2025, 2:56:56 PM	—



Settings for Table

View semantic model

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

Refresh history

Semantic model description

Describe the contents of this semantic model.

Sensitivity label

Classify the sensitivity of this semantic model Learn more

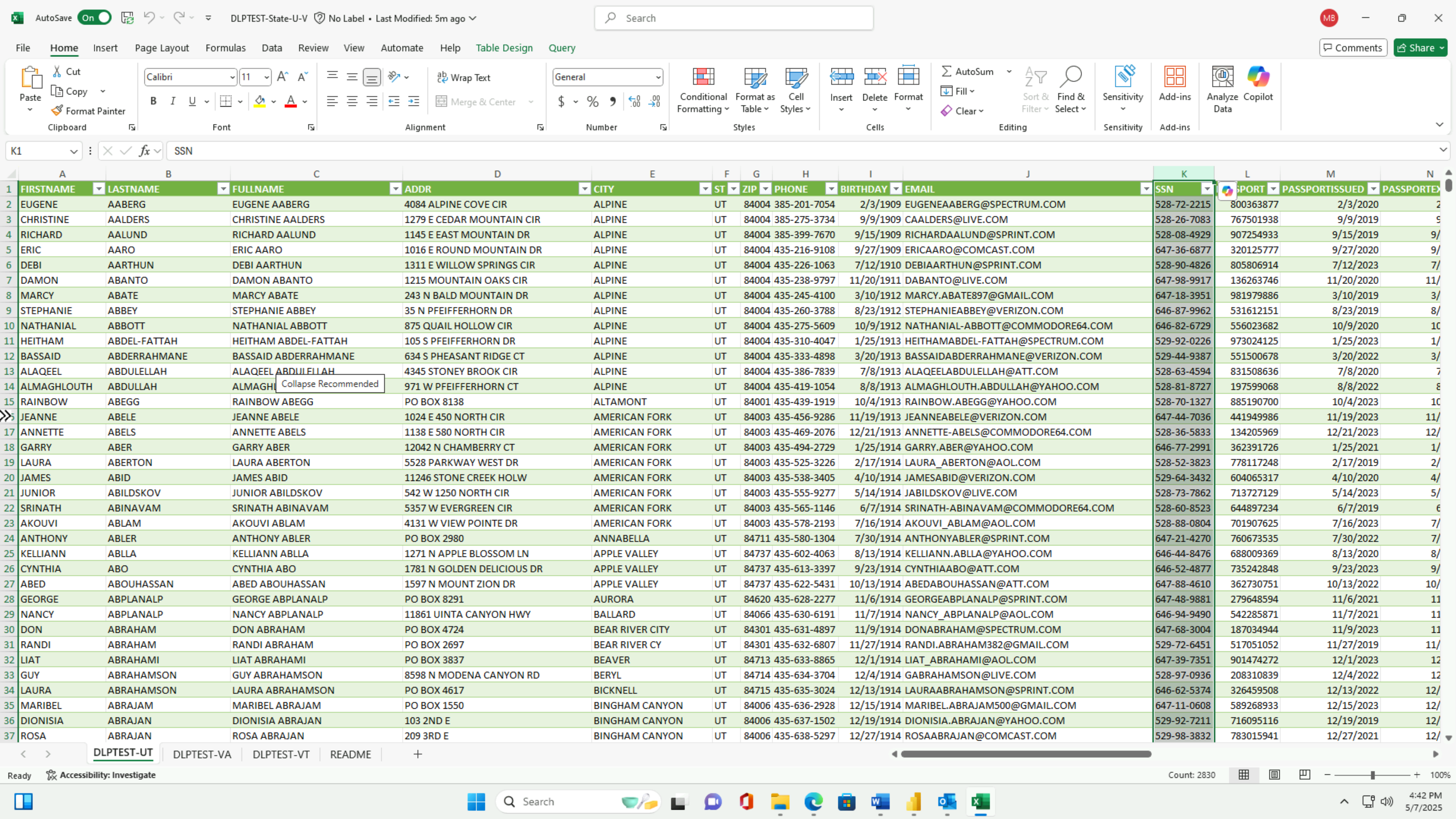
(None)

(None)
Personal
Public
General\Anyone (unrestricted)
General\All Employees (unrestricted)
Confidential\All Employees
Highly Confidential \All Employees
Highly Confidential \DOH Only

tion settings and content marking, are not enforced

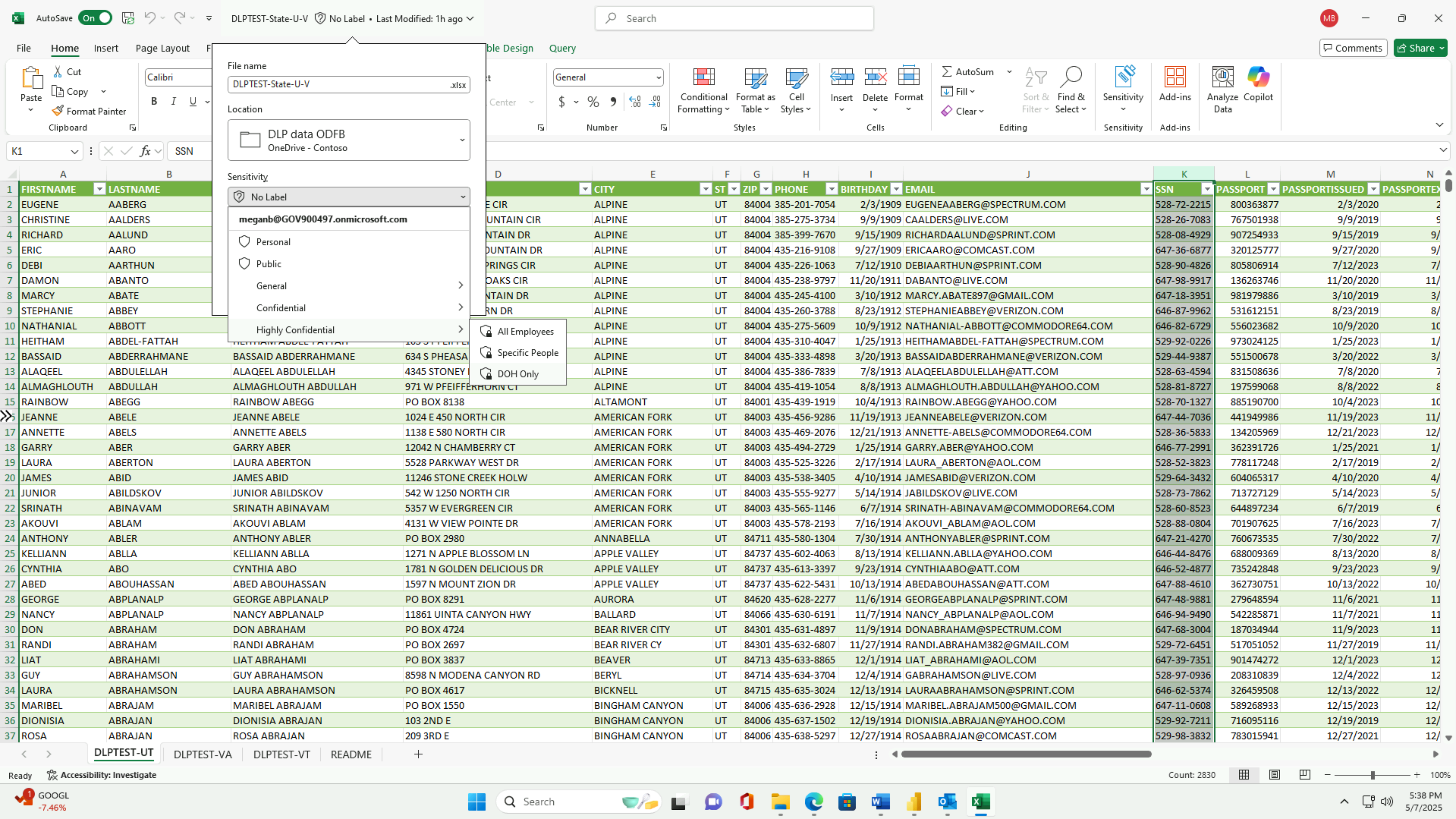
Sensitivity label inheritance from data sources

- Power BI can inherit sensitivity labels from supported data sources like:
    - Excel files stored on OneDrive or SharePoint Online*
    - Azure Synapse Analytics (formerly SQL Data Warehouse)
    - Azure SQL Database



K1 | SSN

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	FIRSTNAME	LASTNAME	FULLNAME	ADDR	CITY	ST	ZIP	PHONE	BIRTHDAY	EMAIL	SSN	SPORT	PASSPORTISSUED	PASSPORTEX
2	EUGENE	AABERG	EUGENE AABERG	4084 ALPINE COVE CIR	ALPINE	UT	84004	385-201-7054	2/3/1909	EUGENEAABERG@SPECTRUM.COM	528-72-2215	800363877	2/3/2020	2
3	CHRISTINE	AALDERS	CHRISTINE AALDERS	1279 E CEDAR MOUNTAIN CIR	ALPINE	UT	84004	385-275-3734	9/9/1909	CAALDERS@LIVE.COM	528-26-7083	767501938	9/9/2019	9
4	RICHARD	AALUND	RICHARD AALUND	1145 E EAST MOUNTAIN DR	ALPINE	UT	84004	385-399-7670	9/15/1909	RICHARDAALUND@SPRINT.COM	528-08-4929	907254933	9/15/2019	9/
5	ERIC	AARO	ERIC AARO	1016 E ROUND MOUNTAIN DR	ALPINE	UT	84004	435-216-9108	9/27/1909	ERICAARO@COMCAST.COM	647-36-6877	320125777	9/27/2020	9/
6	DEBI	AARTHUN	DEBI AARTHUN	1311 E WILLOW SPRINGS CIR	ALPINE	UT	84004	435-226-1063	7/12/1910	DEBIAARTHUN@SPRINT.COM	528-90-4826	805806914	7/12/2023	7/
7	DAMON	ABANTO	DAMON ABANTO	1215 MOUNTAIN OAKS CIR	ALPINE	UT	84004	435-238-9797	11/20/1911	DABANTO@LIVE.COM	647-98-9917	136263746	11/20/2020	11/
8	MARCY	ABATE	MARCY ABATE	243 N BALD MOUNTAIN DR	ALPINE	UT	84004	435-245-4100	3/10/1912	MARCY.ABATE897@GMAIL.COM	647-18-3951	981979886	3/10/2019	3/
9	STEPHANIE	ABBEY	STEPHANIE ABBEY	35 N PFEIFFERHORN DR	ALPINE	UT	84004	435-260-3788	8/23/1912	STEPHANIEABBEY@VERIZON.COM	646-87-9962	531612151	8/23/2019	8/
10	NATHANIAL	ABBOTT	NATHANIAL ABBOTT	875 QUAIL HOLLOW CIR	ALPINE	UT	84004	435-275-5609	10/9/1912	NATHANIAL-ABBOTT@COMMODORE64.COM	646-82-6729	556023682	10/9/2020	10
11	HEITHAM	ABDEL-FATTAH	HEITHAM ABDEL-FATTAH	105 S PFEIFFERHORN DR	ALPINE	UT	84004	435-310-4047	1/25/1913	HEITHAMABDEL-FATTAH@SPECTRUM.COM	529-92-0226	973024125	1/25/2023	1/
12	BASSAID	ABDERRAHMANE	BASSAID ABDERRAHMANE	634 S PHEASANT RIDGE CT	ALPINE	UT	84004	435-333-4898	3/20/1913	BASSAIDABDERRAHMANE@VERIZON.COM	529-44-9387	551500678	3/20/2022	3/
13	ALAQEEL	ABDULELLAH	ALAQEEL ABDULELLAH	4345 STONEY BROOK CIR	ALPINE	UT	84004	435-386-7839	7/8/1913	ALAQEELABDULELLAH@ATT.COM	528-63-4594	831508636	7/8/2020	7
14	ALMAGHLOUTH	ABDULLAH	ALMAGHI	971 W PFEIFFERHORN CT	ALPINE	UT	84004	435-419-1054	8/8/1913	ALMAGHLOUTH.ABDULLAH@YAHOO.COM	528-81-8727	197599068	8/8/2022	8
15	RAINBOW	ABEGG	RAINBOW ABEGG	PO BOX 8138	ALTAMONT	UT	84001	435-439-1919	10/4/1913	RAINBOW.ABEGG@YAHOO.COM	528-70-1327	885190700	10/4/2023	10
16	JEANNE	ABELE	JEANNE ABELE	1024 E 450 NORTH CIR	AMERICAN FORK	UT	84003	435-456-9286	11/19/1913	JEANNEABELE@VERIZON.COM	647-44-7036	441949986	11/19/2023	11/
17	ANNETTE	ABELS	ANNETTE ABELS	1138 E 580 NORTH CIR	AMERICAN FORK	UT	84003	435-469-2076	12/21/1913	ANNETTE-ABELS@COMMODORE64.COM	528-36-5833	134205969	12/21/2023	12/
18	GARRY	ABER	GARRY ABER	12042 N CHAMBERRY CT	AMERICAN FORK	UT	84003	435-494-2729	1/25/1914	GARRY.ABER@YAHOO.COM	646-77-2991	362391726	1/25/2021	1/
19	LAURA	ABERTON	LAURA ABERTON	5528 PARKWAY WEST DR	AMERICAN FORK	UT	84003	435-525-3226	2/17/1914	LAURA_ABERTON@AOL.COM	528-52-3823	778117248	2/17/2019	2/
20	JAMES	ABID	JAMES ABID	11246 STONE CREEK HOLW	AMERICAN FORK	UT	84003	435-538-3405	4/10/1914	JAMESABID@VERIZON.COM	529-64-3432	604065317	4/10/2020	4/
21	JUNIOR	ABILDSKOV	JUNIOR ABILDSKOV	542 W 1250 NORTH CIR	AMERICAN FORK	UT	84003	435-555-9277	5/14/1914	JABILDSKOV@LIVE.COM	528-73-7862	713727129	5/14/2023	5/
22	SRINATH	ABINAVAM	SRINATH ABINAVAM	5357 W EVERGREEN CIR	AMERICAN FORK	UT	84003	435-565-1146	6/7/1914	SRINATH-ABINAVAM@COMMODORE64.COM	528-60-8523	644897234	6/7/2019	6
23	AKOUVI	ABLAM	AKOUVI ABLAM	4131 W VIEW POINTE DR	AMERICAN FORK	UT	84003	435-578-2193	7/16/1914	AKOUVI_ABLAM@AOL.COM	528-88-0804	701907625	7/16/2023	7/
24	ANTHONY	ABLER	ANTHONY ABLER	PO BOX 2980	ANNABELLA	UT	84711	435-580-1304	7/30/1914	ANTHONYABLER@SPRINT.COM	647-21-4270	760673535	7/30/2022	7/
25	KELLIANN	ABLLA	KELLIANN ABLLA	1271 N APPLE BLOSSOM LN	APPLE VALLEY	UT	84737	435-602-4063	8/13/1914	KELLIANN.ABLLA@YAHOO.COM	646-44-8476	688009369	8/13/2020	8/
26	CYNTHIA	ABO	CYNTHIA ABO	1781 N GOLDEN DELICIOUS DR	APPLE VALLEY	UT	84737	435-613-3397	9/23/1914	CYNTHIAABO@ATT.COM	646-52-4877	735242848	9/23/2023	9/
27	ABED	ABOUHASSAN	ABED ABOUHASSAN	1597 N MOUNT ZION DR	APPLE VALLEY	UT	84737	435-622-5431	10/13/1914	ABEDABOUHASSAN@ATT.COM	647-88-4610	362730751	10/13/2022	10/
28	GEORGE	ABPLANALP	GEORGE ABPLANALP	PO BOX 8291	AURORA	UT	84620	435-628-2277	11/6/1914	GEORGEABPLANALP@SPRINT.COM	647-48-9881	279648594	11/6/2021	11
29	NANCY	ABPLANALP	NANCY ABPLANALP	11861 UINTA CANYON HWY	BALLARD	UT	84066	435-630-6191	11/7/1914	NANCY_ABPLANALP@AOL.COM	646-94-9490	542285871	11/7/2021	11
30	DON	ABRAHAM	DON ABRAHAM	PO BOX 4724	BEAR RIVER CITY	UT	84301	435-631-4897	11/9/1914	DONABRAHAM@SPECTRUM.COM	647-68-3004	187034944	11/9/2023	11
31	RANDI	ABRAHAM	RANDI ABRAHAM	PO BOX 2697	BEAR RIVER CY	UT	84301	435-632-6807	11/27/1914	RANDI.ABRAHAM382@GMAIL.COM	529-72-6451	517051052	11/27/2019	11/
32	LIAT	ABRAHAMI	LIAT ABRAHAMI	PO BOX 3837	BEAVER	UT	84713	435-633-8865	12/1/1914	LIAT_ABRAHAMI@AOL.COM	647-39-7351	901474272	12/1/2023	12
33	GUY	ABRAHAMSON	GUY ABRAHAMSON	8598 N MODENA CANYON RD	BERYL	UT	84714	435-634-3704	12/4/1914	GABRAHAMSON@LIVE.COM	528-97-0936	208310839	12/4/2022	12
34	LAURA	ABRAHAMSON	LAURA ABRAHAMSON	PO BOX 4617	BICKNELL	UT	84715	435-635-3024	12/13/1914	LAURAABRAHAMSON@SPRINT.COM	646-62-5374	326459508	12/13/2022	12/
35	MARIBEL	ABRAJAM	MARIBEL ABRAJAM	PO BOX 1550	BINGHAM CANYON	UT	84006	435-636-2928	12/15/1914	MARIBEL.ABRAJAM500@GMAIL.COM	647-11-0608	589268933	12/15/2023	12/
36	DIONISIA	ABRAJAN	DIONISIA ABRAJAN	103 2ND E	BINGHAM CANYON	UT	84006	435-637-1502	12/19/1914	DIONISIA.ABRAJAN@YAHOO.COM	529-92-7211	716095116	12/19/2019	12/
37	ROSA	ABRAJAN	ROSA ABRAJAN	209 3RD E	BINGHAM CANYON	UT	84006	435-638-5297	12/27/1914	ROSAABRAJAN@COMCAST.COM	529-98-3832	783015941	12/27/2021	12/

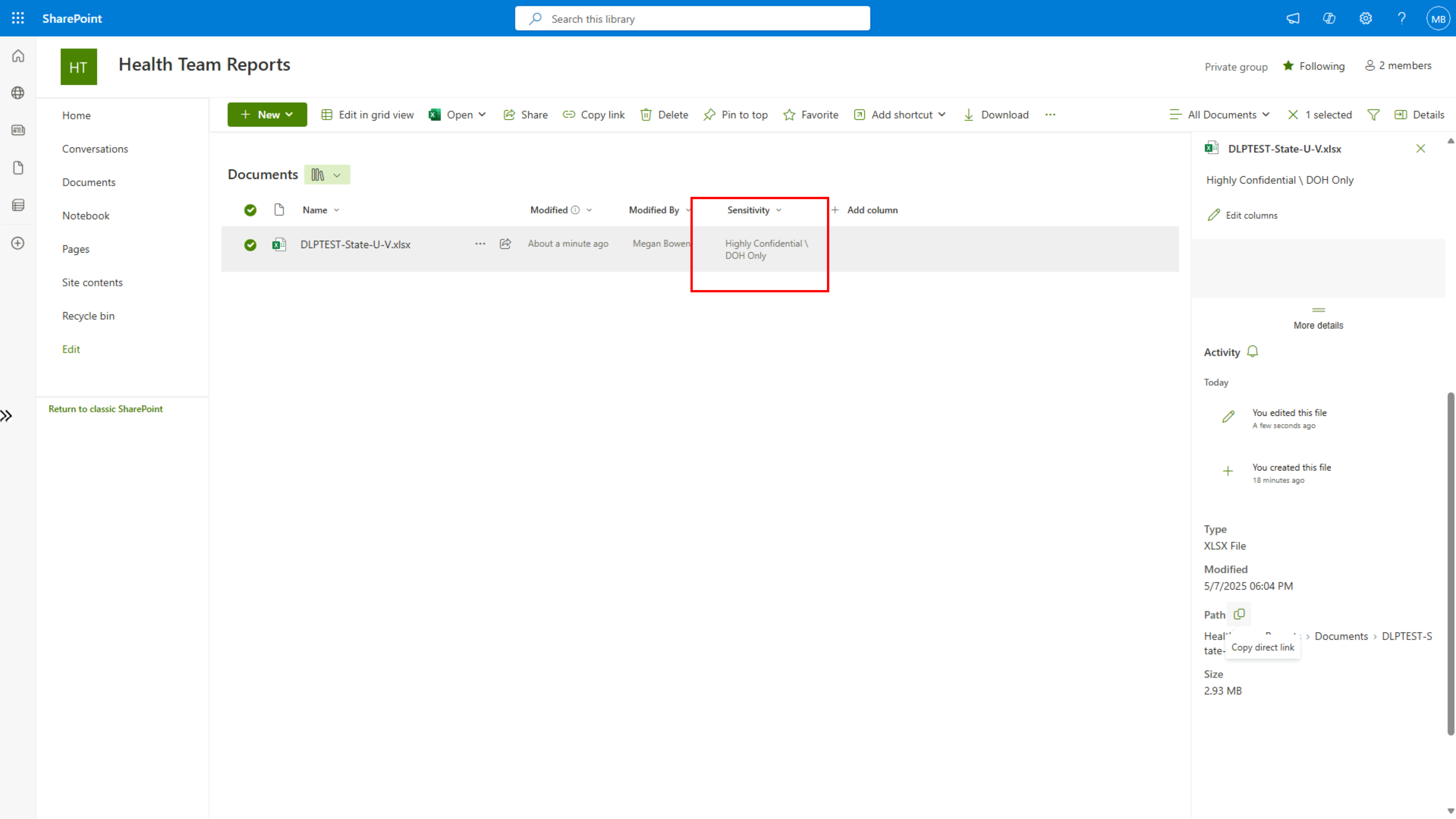


File name: DLPTEST-State-U-V .xlsx

Location: DLP data ODFB — OneDrive - Contoso

Sensitivity: No Label

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	FIRSTNAME	LASTNAME			CITY	ST	ZIP	PHONE	BIRTHDAY	EMAIL	SSN	PASSPORT	PASSPORTISSUED	PASSPORTEX
2	EUGENE	AABERG		E CIR	ALPINE	UT	84004	385-201-7054	2/3/1909	EUGENEAABERG@SPECTRUM.COM	528-72-2215	800363877	2/3/2020	2
3	CHRISTINE	AALDERS		UNTAIN CIR	ALPINE	UT	84004	385-275-3734	9/9/1909	CAALDERS@LIVE.COM	528-26-7083	767501938	9/9/2019	9
4	RICHARD	AALUND		NTAIN DR	ALPINE	UT	84004	385-399-7670	9/15/1909	RICHARDAALUND@SPRINT.COM	528-08-4929	907254933	9/15/2019	9/
5	ERIC	AARO		OUNTAIN DR	ALPINE	UT	84004	435-216-9108	9/27/1909	ERICAARO@COMCAST.COM	647-36-6877	320125777	9/27/2020	9/
6	DEBI	AARTHUN		PRINGS CIR	ALPINE	UT	84004	435-226-1063	7/12/1910	DEBIAARTHUN@SPRINT.COM	528-90-4826	805806914	7/12/2023	7/
7	DAMON	ABANTO		OAKS CIR	ALPINE	UT	84004	435-238-9797	11/20/1911	DABANTO@LIVE.COM	647-98-9917	136263746	11/20/2020	11/
8	MARCY	ABATE		NTAIN DR	ALPINE	UT	84004	435-245-4100	3/10/1912	MARCY.ABATE897@GMAIL.COM	647-18-3951	981979886	3/10/2019	3/
9	STEPHANIE	ABBEY		RN DR	ALPINE	UT	84004	435-260-3788	8/23/1912	STEPHANIEABBEY@VERIZON.COM	646-87-9962	531612151	8/23/2019	8/
10	NATHANIAL	ABBOTT			ALPINE	UT	84004	435-275-5609	10/9/1912	NATHANIAL-ABBOTT@COMMODORE64.COM	646-82-6729	556023682	10/9/2020	10
11	HEITHAM	ABDEL-FATTAH	HEITHAM ABDEL-FATTAH	165 S PFEIFFE	ALPINE	UT	84004	435-310-4047	1/25/1913	HEITHAMABDEL-FATTAH@SPECTRUM.COM	529-92-0226	973024125	1/25/2023	1/
12	BASSAID	ABDERRAHMANE	BASSAID ABDERRAHMANE	634 S PHEASA	ALPINE	UT	84004	435-333-4898	3/20/1913	BASSAIDABDERRAHMANE@VERIZON.COM	529-44-9387	551500678	3/20/2022	3/
13	ALAQEEL	ABDULELLAH	ALAQEEL ABDULELLAH	4345 STONEY I	ALPINE	UT	84004	435-386-7839	7/8/1913	ALAQEELABDULELLAH@ATT.COM	528-63-4594	831508636	7/8/2020	7
14	ALMAGHLOUTH	ABDULLAH	ALMAGHLOUTH ABDULLAH	971 W PFEIFFERHORN CT	ALPINE	UT	84004	435-419-1054	8/8/1913	ALMAGHLOUTH.ABDULLAH@YAHOO.COM	528-81-8727	197599068	8/8/2022	8
15	RAINBOW	ABEGG	RAINBOW ABEGG	PO BOX 8138	ALTAMONT	UT	84001	435-439-1919	10/4/1913	RAINBOW.ABEGG@YAHOO.COM	528-70-1327	885190700	10/4/2023	10
16	JEANNE	ABELE	JEANNE ABELE	1024 E 450 NORTH CIR	AMERICAN FORK	UT	84003	435-456-9286	11/19/1913	JEANNEABELE@VERIZON.COM	647-44-7036	441949986	11/19/2023	11/
17	ANNETTE	ABELS	ANNETTE ABELS	1138 E 580 NORTH CIR	AMERICAN FORK	UT	84003	435-469-2076	12/21/1913	ANNETTE-ABELS@COMMODORE64.COM	528-36-5833	134205969	12/21/2023	12/
18	GARRY	ABER	GARRY ABER	12042 N CHAMBERRY CT	AMERICAN FORK	UT	84003	435-494-2729	1/25/1914	GARRY.ABER@YAHOO.COM	646-77-2991	362391726	1/25/2021	1/
19	LAURA	ABERTON	LAURA ABERTON	5528 PARKWAY WEST DR	AMERICAN FORK	UT	84003	435-525-3226	2/17/1914	LAURA_ABERTON@AOL.COM	528-52-3823	778117248	2/17/2019	2/
20	JAMES	ABID	JAMES ABID	11246 STONE CREEK HOLW	AMERICAN FORK	UT	84003	435-538-3405	4/10/1914	JAMESABID@VERIZON.COM	529-64-3432	604065317	4/10/2020	4/
21	JUNIOR	ABILDSKOV	JUNIOR ABILDSKOV	542 W 1250 NORTH CIR	AMERICAN FORK	UT	84003	435-555-9277	5/14/1914	JABILDSKOV@LIVE.COM	528-73-7862	713727129	5/14/2023	5/
22	SRINATH	ABINAVAM	SRINATH ABINAVAM	5357 W EVERGREEN CIR	AMERICAN FORK	UT	84003	435-565-1146	6/7/1914	SRINATH-ABINAVAM@COMMODORE64.COM	528-60-8523	644897234	6/7/2019	6
23	AKOUVI	ABLAM	AKOUVI ABLAM	4131 W VIEW POINTE DR	AMERICAN FORK	UT	84003	435-578-2193	7/16/1914	AKOUVI_ABLAM@AOL.COM	528-88-0804	701907625	7/16/2023	7/
24	ANTHONY	ABLER	ANTHONY ABLER	PO BOX 2980	ANNABELLA	UT	84711	435-580-1304	7/30/1914	ANTHONYABLER@SPRINT.COM	647-21-4270	760673535	7/30/2022	7/
25	KELLIANN	ABLLA	KELLIANN ABLLA	1271 N APPLE BLOSSOM LN	APPLE VALLEY	UT	84737	435-602-4063	8/13/1914	KELLIANN.ABLLA@YAHOO.COM	646-44-8476	688009369	8/13/2020	8/
26	CYNTHIA	ABO	CYNTHIA ABO	1781 N GOLDEN DELICIOUS DR	APPLE VALLEY	UT	84737	435-613-3397	9/23/1914	CYNTHIAABO@ATT.COM	646-52-4877	735242848	9/23/2023	9/
27	ABED	ABOUHASSAN	ABED ABOUHASSAN	1597 N MOUNT ZION DR	APPLE VALLEY	UT	84737	435-622-5431	10/13/1914	ABEDABOUHASSAN@ATT.COM	647-88-4610	362730751	10/13/2022	10/
28	GEORGE	ABPLANALP	GEORGE ABPLANALP	PO BOX 8291	AURORA	UT	84620	435-628-2277	11/6/1914	GEORGEABPLANALP@SPRINT.COM	647-48-9881	279648594	11/6/2021	11
29	NANCY	ABPLANALP	NANCY ABPLANALP	11861 UINTA CANYON HWY	BALLARD	UT	84066	435-630-6191	11/7/1914	NANCY_ABPLANALP@AOL.COM	646-94-9490	542285871	11/7/2021	11
30	DON	ABRAHAM	DON ABRAHAM	PO BOX 4724	BEAR RIVER CITY	UT	84301	435-631-4897	11/9/1914	DONABRAHAM@SPECTRUM.COM	647-68-3004	187034944	11/9/2023	11
31	RANDI	ABRAHAM	RANDI ABRAHAM	PO BOX 2697	BEAR RIVER CY	UT	84301	435-632-6807	11/27/1914	RANDI.ABRAHAM382@GMAIL.COM	529-72-6451	517051052	11/27/2019	11/
32	LIAT	ABRAHAMI	LIAT ABRAHAMI	PO BOX 3837	BEAVER	UT	84713	435-633-8865	12/1/1914	LIAT_ABRAHAMI@AOL.COM	647-39-7351	901474272	12/1/2023	12
33	GUY	ABRAHAMSON	GUY ABRAHAMSON	8598 N MODENA CANYON RD	BERYL	UT	84714	435-634-3704	12/4/1914	GABRAHAMSON@LIVE.COM	528-97-0936	208310839	12/4/2022	12
34	LAURA	ABRAHAMSON	LAURA ABRAHAMSON	PO BOX 4617	BICKNELL	UT	84715	435-635-3024	12/13/1914	LAURAABRAHAMSON@SPRINT.COM	646-62-5374	326459508	12/13/2022	12/
35	MARIBEL	ABRAJAM	MARIBEL ABRAJAM	PO BOX 1550	BINGHAM CANYON	UT	84006	435-636-2928	12/15/1914	MARIBEL.ABRAJAM500@GMAIL.COM	647-11-0608	589268933	12/15/2023	12/
36	DIONISIA	ABRAJAN	DIONISIA ABRAJAN	103 2ND E	BINGHAM CANYON	UT	84006	435-637-1502	12/19/1914	DIONISIA.ABRAJAN@YAHOO.COM	529-92-7211	716095116	12/19/2019	12/
37	ROSA	ABRAJAN	ROSA ABRAJAN	209 3RD E	BINGHAM CANYON	UT	84006	435-638-5297	12/27/1914	ROSAABRAJAN@COMCAST.COM	529-98-3832	783015941	12/27/2021	12/



SharePoint

Search this library

HT Health Team Reports

Private group · Following · 2 members

Home
Conversations
Documents
Notebook
Pages
Site contents
Recycle bin
Edit

Return to classic SharePoint

+ New · Edit in grid view · Open · Share · Copy link · Delete · Pin to top · Favorite · Add shortcut · Download · ··· · All Documents · 1 selected · Details

Documents

Name	Modified	Modified By	Sensitivity	+ Add column
DLPTEST-State-U-V.xlsx	About a minute ago	Megan Bowen	Highly Confidential \ DOH Only	

DLPTEST-State-U-V.xlsx

Highly Confidential \ DOH Only

Edit columns

More details

Activity

Today

You edited this file
A few seconds ago

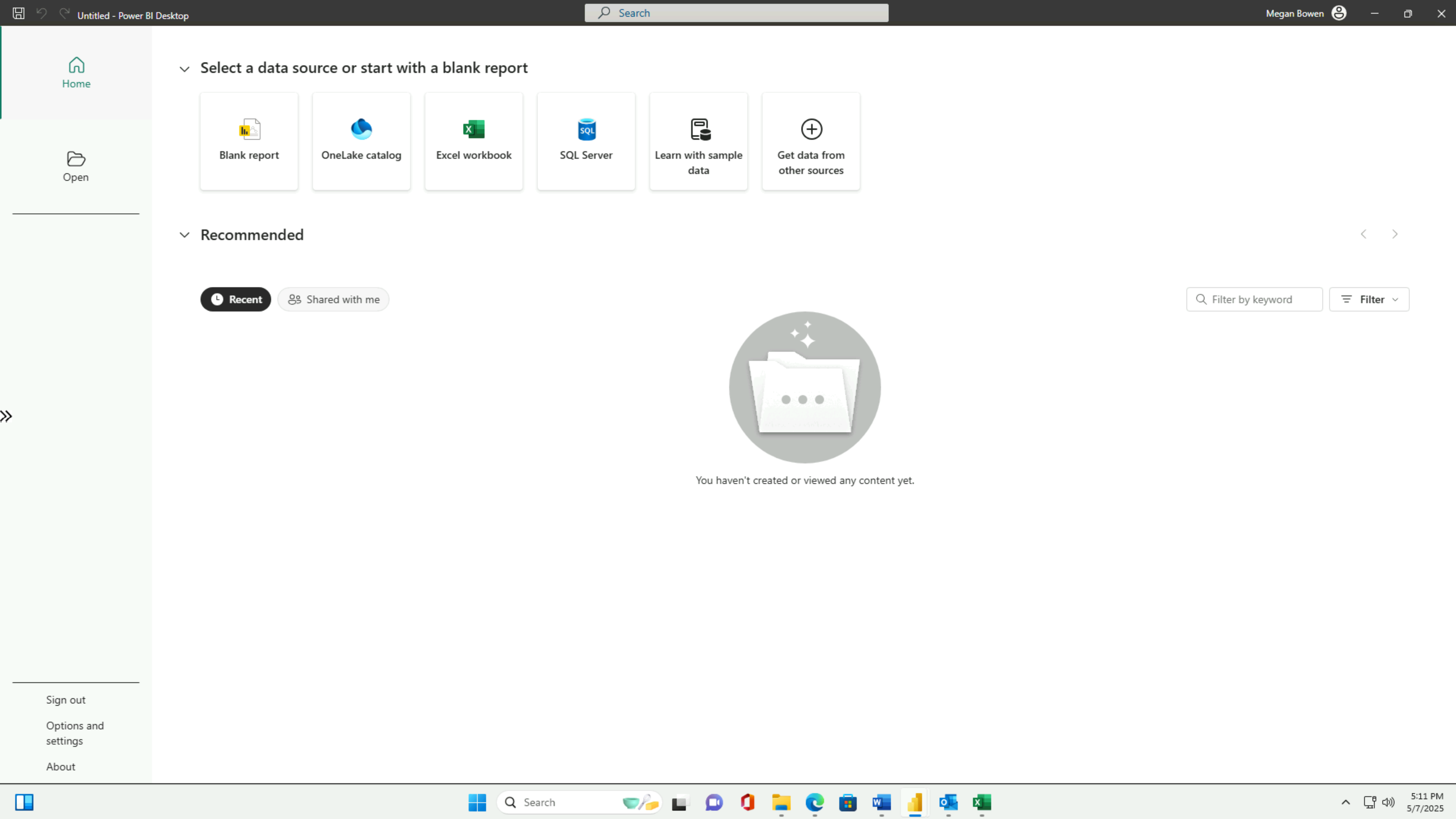
You created this file
18 minutes ago

Type
XLSX File

Modified
5/7/2025 06:04 PM

Path
Heal… > Documents > DLPTEST-State-…
Copy direct link

Size
2.93 MB

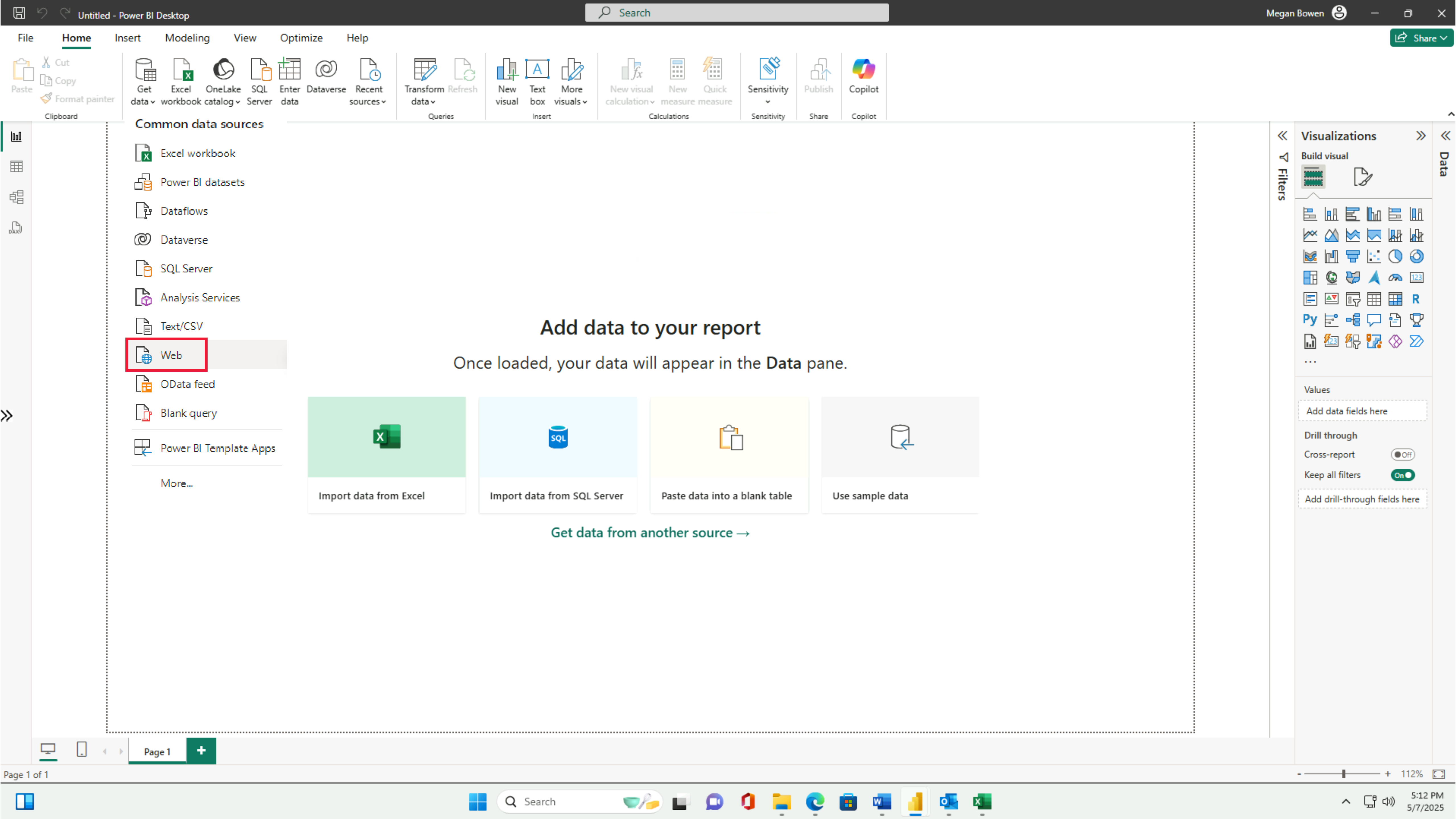


Untitled - Power BI Desktop

Select a data source or start with a blank report

Recommended

You haven't created or viewed any content yet.



Add data to your report

Once loaded, your data will appear in the **Data** pane.

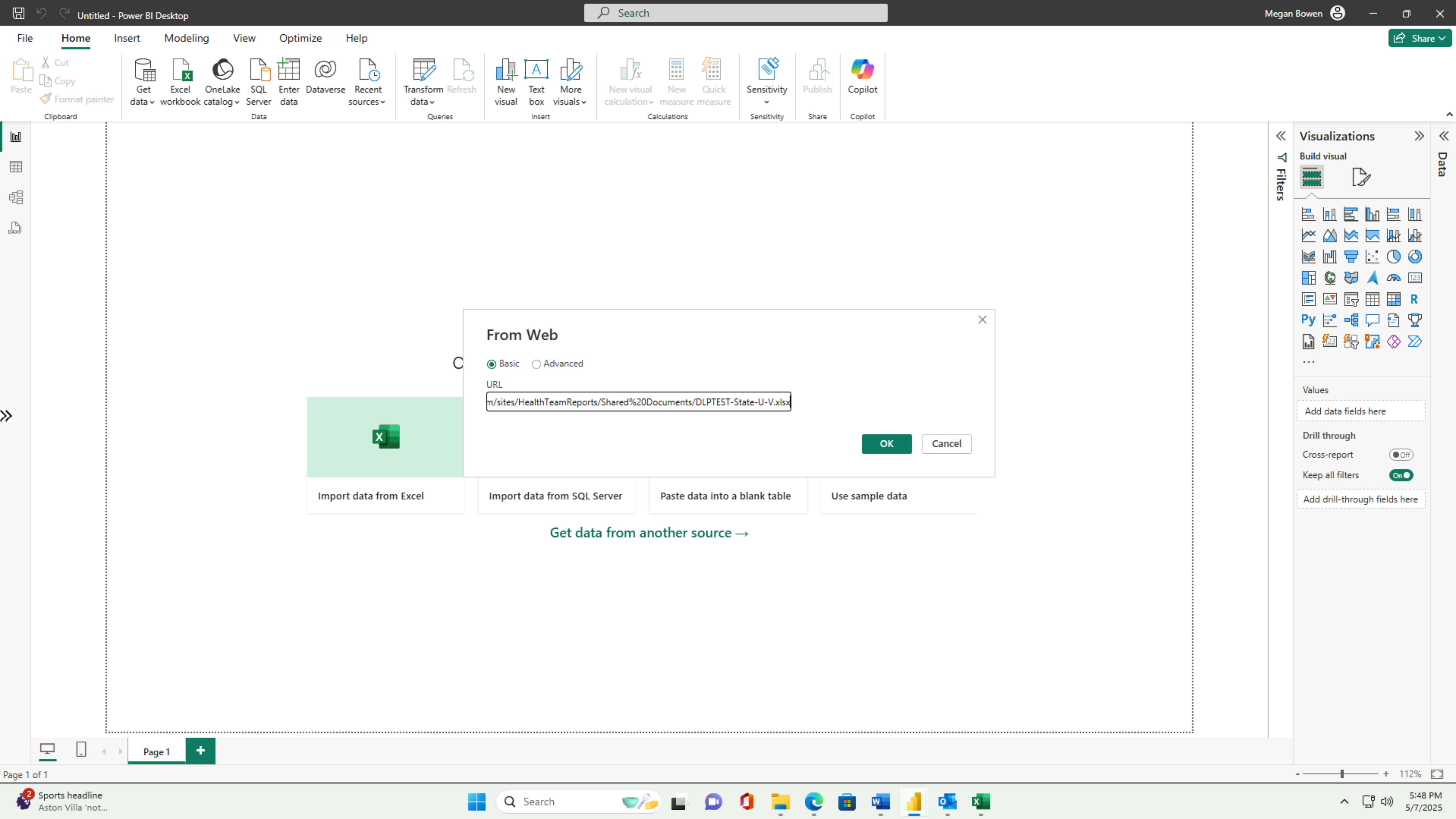
Import data from Excel

Import data from SQL Server

Paste data into a blank table

Use sample data

Get data from another source →



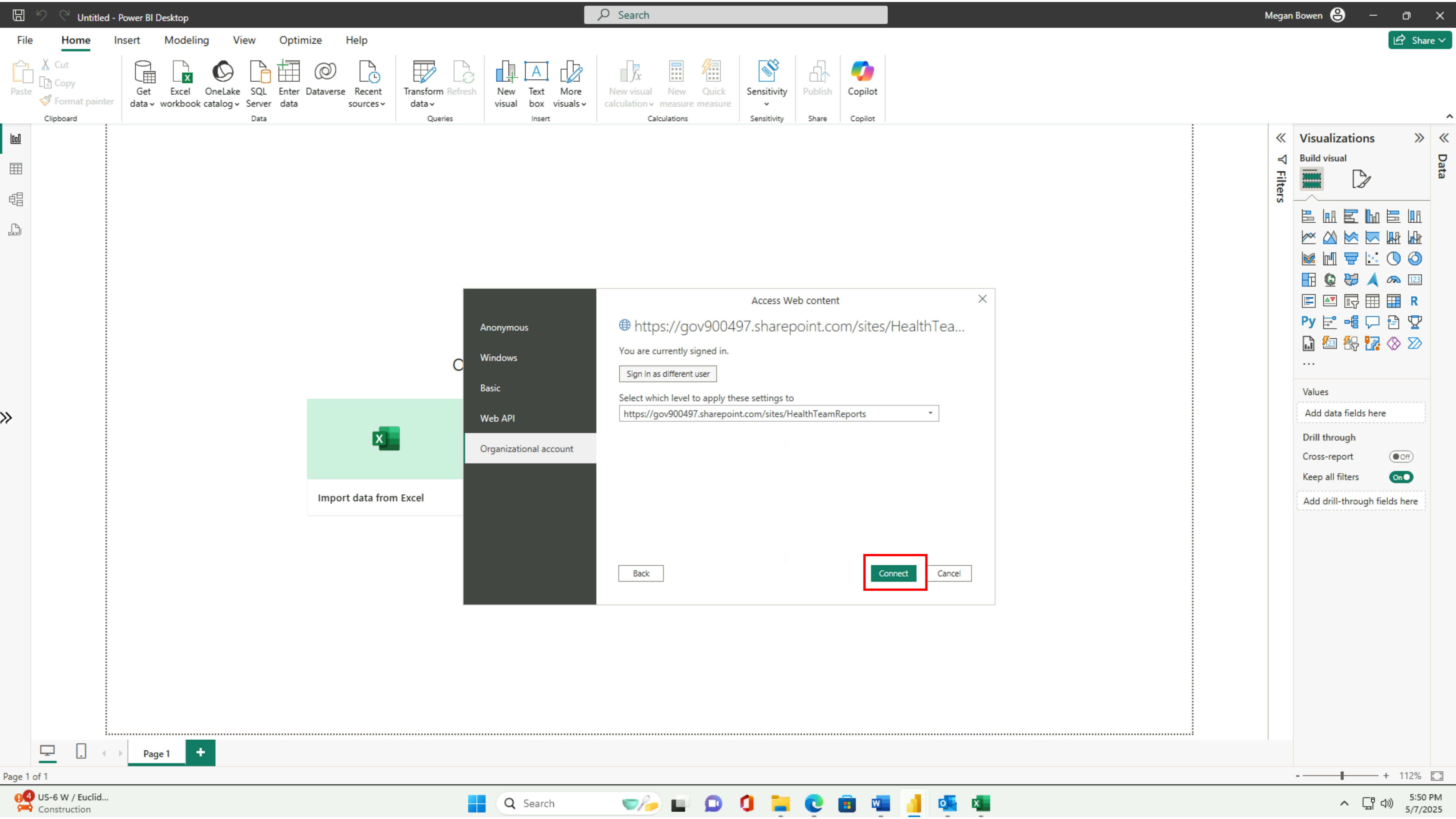
From Web

● Basic ○ Advanced

URL

m/sites/HealthTeamReports/Shared%20Documents/DLPTEST-State-U-V.xlsx

OK Cancel



Access Web content

https://gov900497.sharepoint.com/sites/HealthTea...

You are currently signed in.

Sign in as different user

Select which level to apply these settings to

https://gov900497.sharepoint.com/sites/HealthTeamReports

Anonymous

Windows

Basic

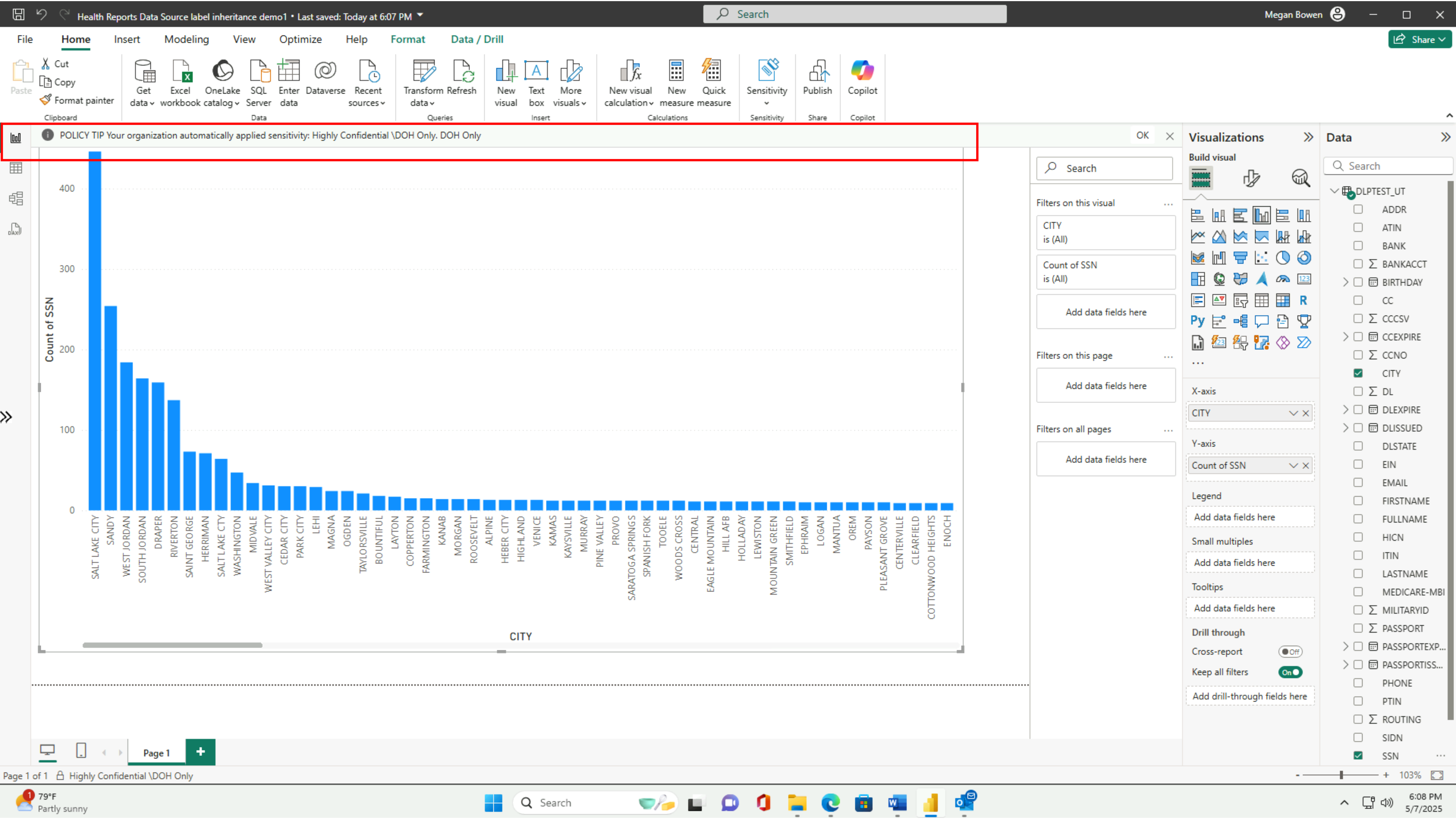
Web API

Organizational account

Back

Connect

Cancel



Health Reports Data Source label inheritance demo1 • Last saved: Today at 6:07 PM

POLICY TIP Your organization automatically applied sensitivity: Highly Confidential \DOH Only. DOH Only

Filters on this visual

CITY
is (All)

Count of SSN
is (All)

X-axis

CITY

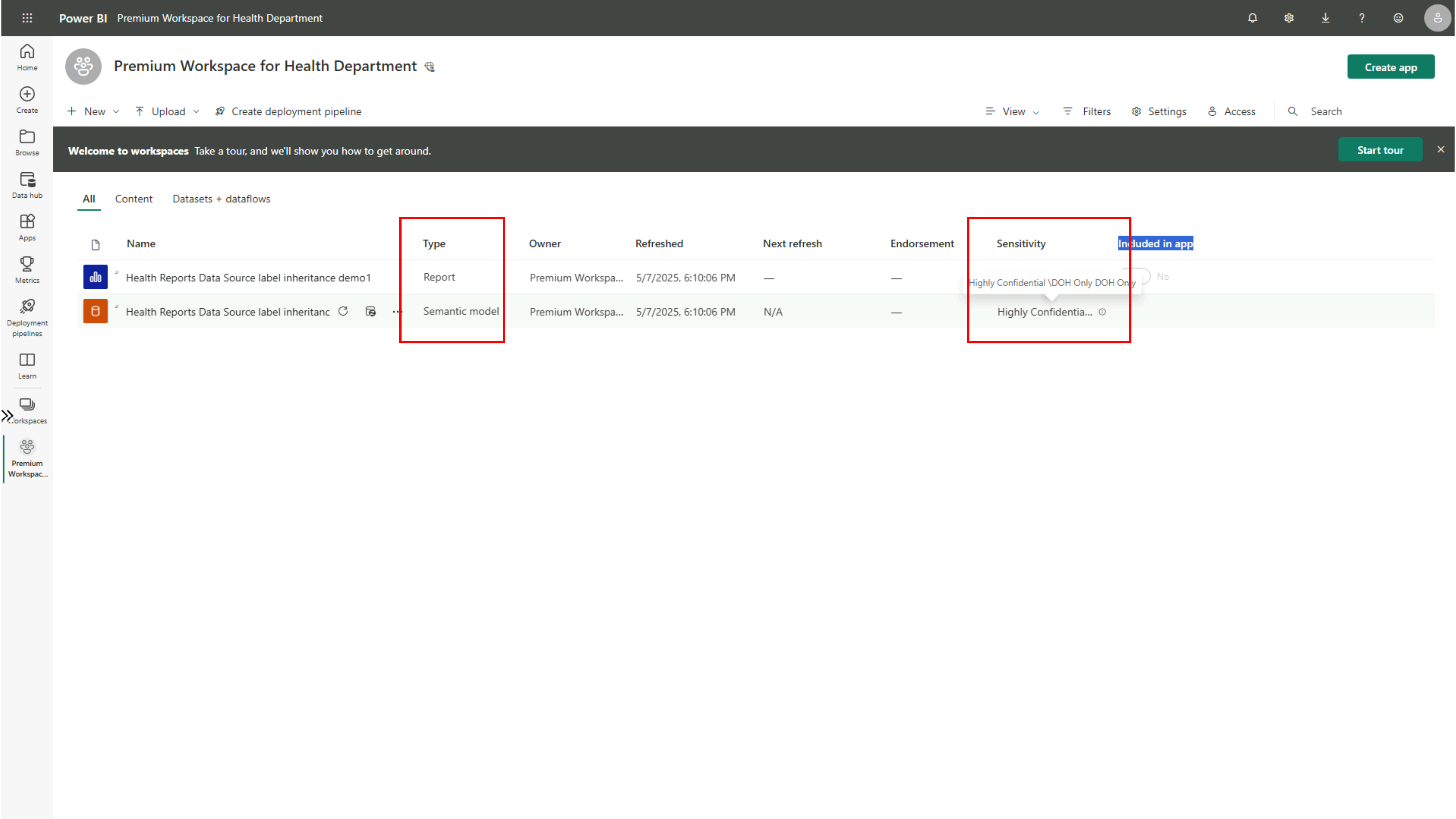
Y-axis

Count of SSN

Cross-report Off

Keep all filters On

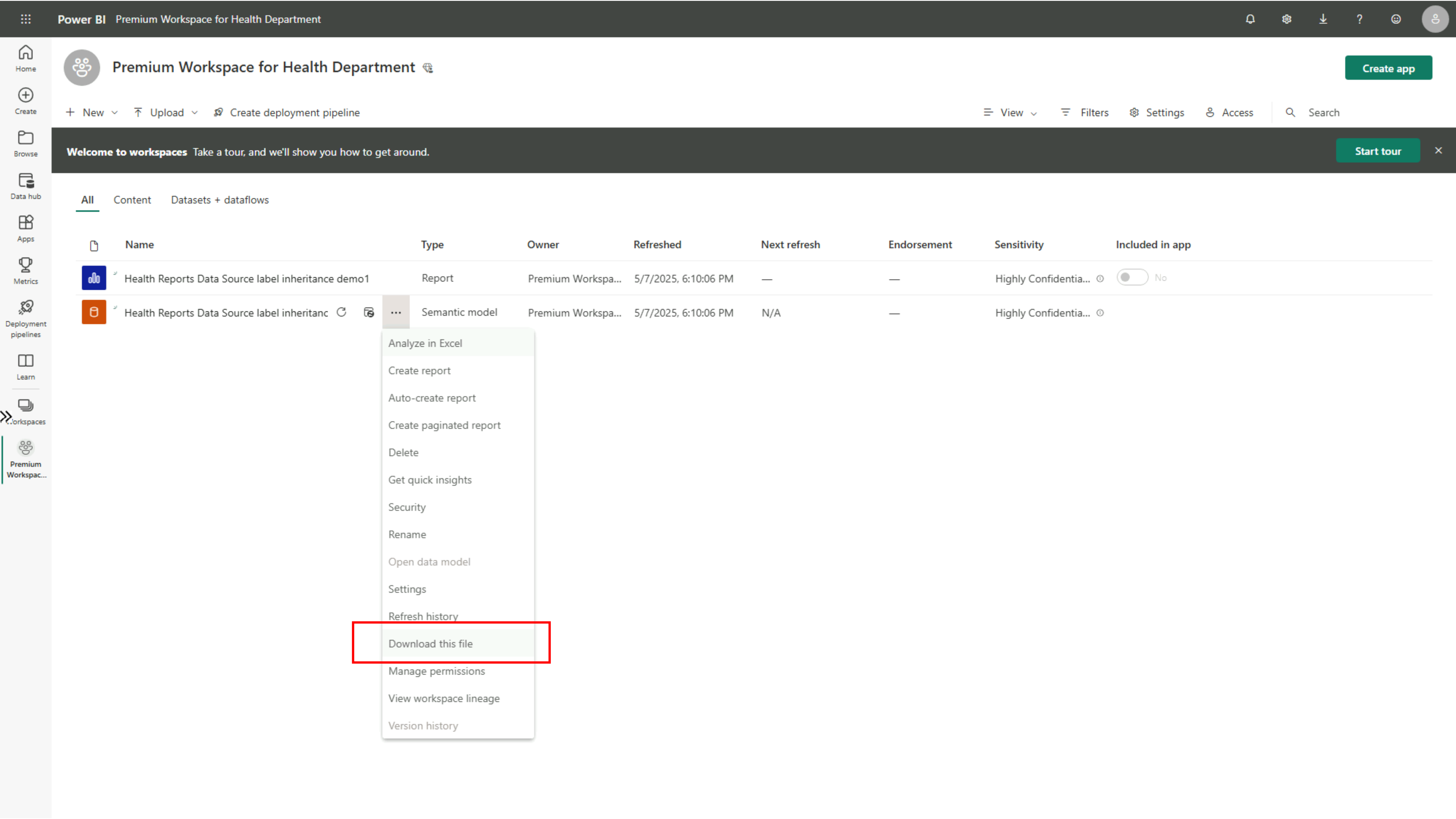
Page 1 of 1 Highly Confidential \DOH Only



Premium Workspace for Health Department

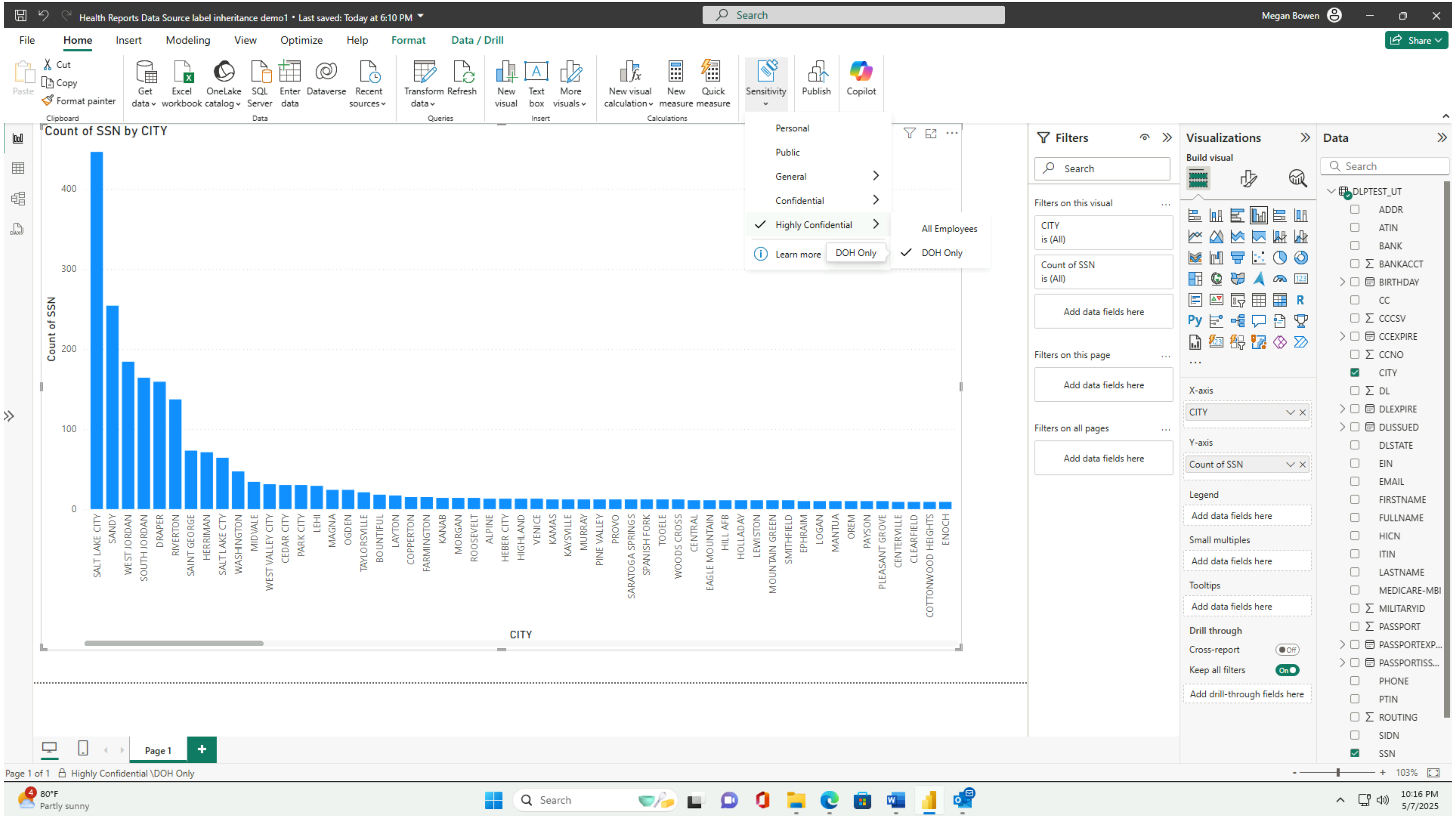
Welcome to workspaces Take a tour, and we'll show you how to get around.

	Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Included in app
	Health Reports Data Source label inheritance demo1	Report	Premium Workspa...	5/7/2025, 6:10:06 PM	—	—	Highly Confidential \DOH Only DOH Only	No
	Health Reports Data Source label inheritanc	Semantic model	Premium Workspa...	5/7/2025, 6:10:06 PM	N/A	—	Highly Confidentia...	



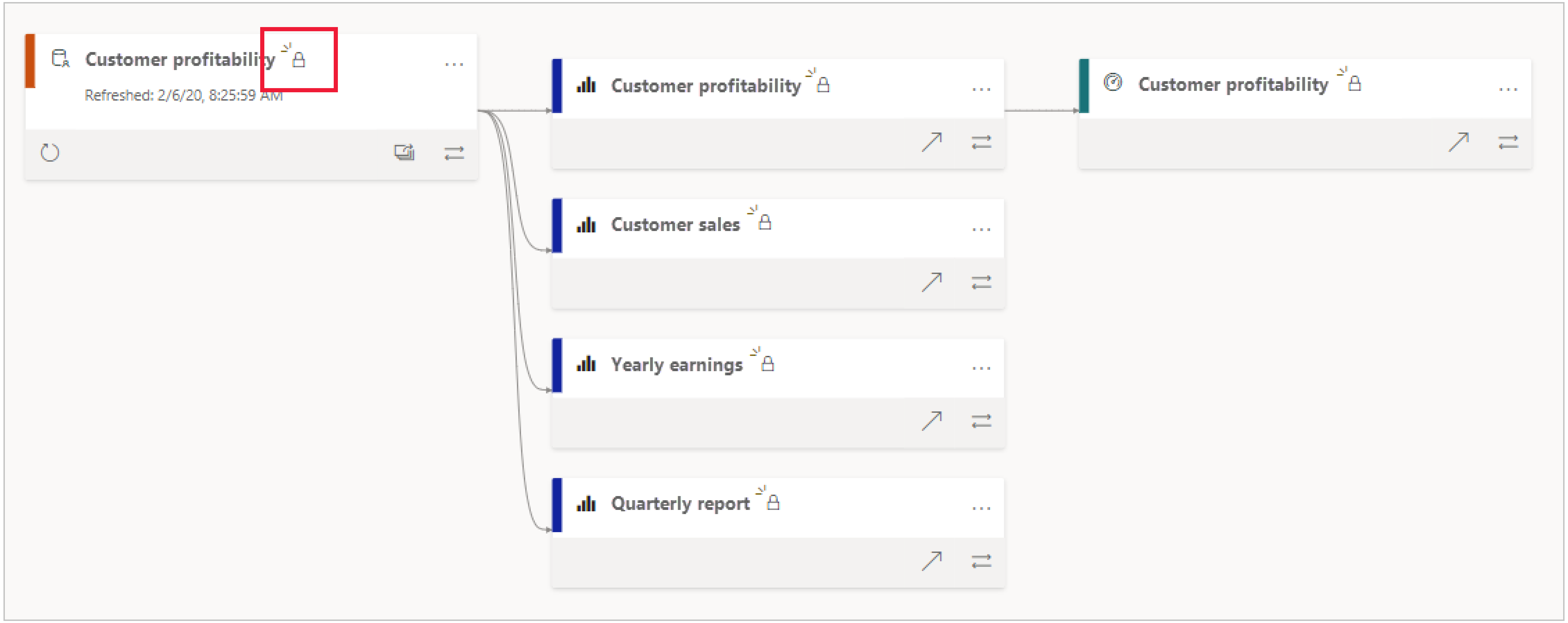
Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Included in app
Health Reports Data Source label inheritance demo1	Report	Premium Workspa...	5/7/2025, 6:10:06 PM	—	—	Highly Confidentia...	No
Health Reports Data Source label inheritanc	Semantic model	Premium Workspa...	5/7/2025, 6:10:06 PM	N/A	—	Highly Confidentia...	

Apply sensitivity labels in Power BI Desktop

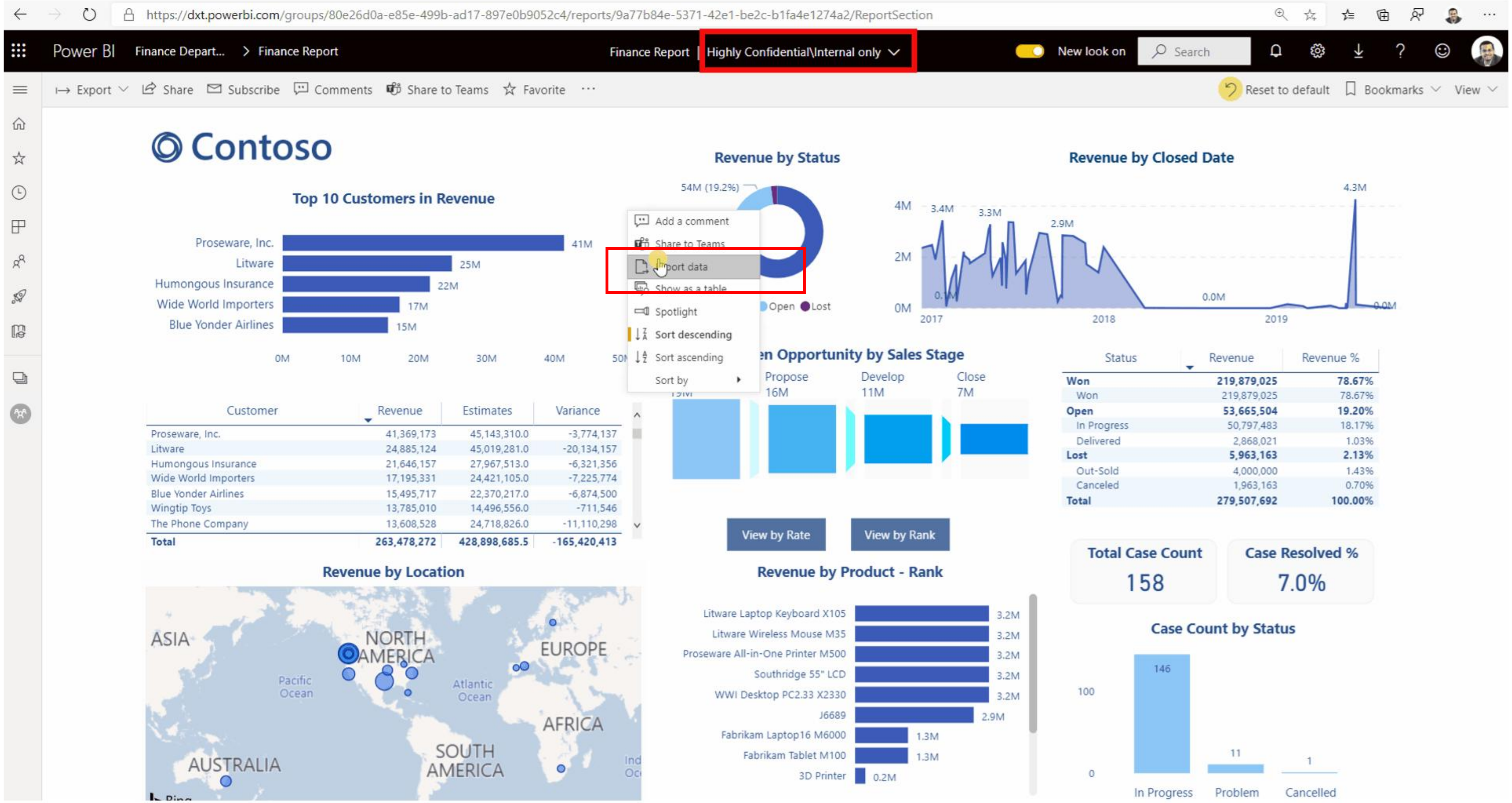


Sensitivity label downstream inheritance

Downstream inheritance



Sensitivity labels and protection on exported data



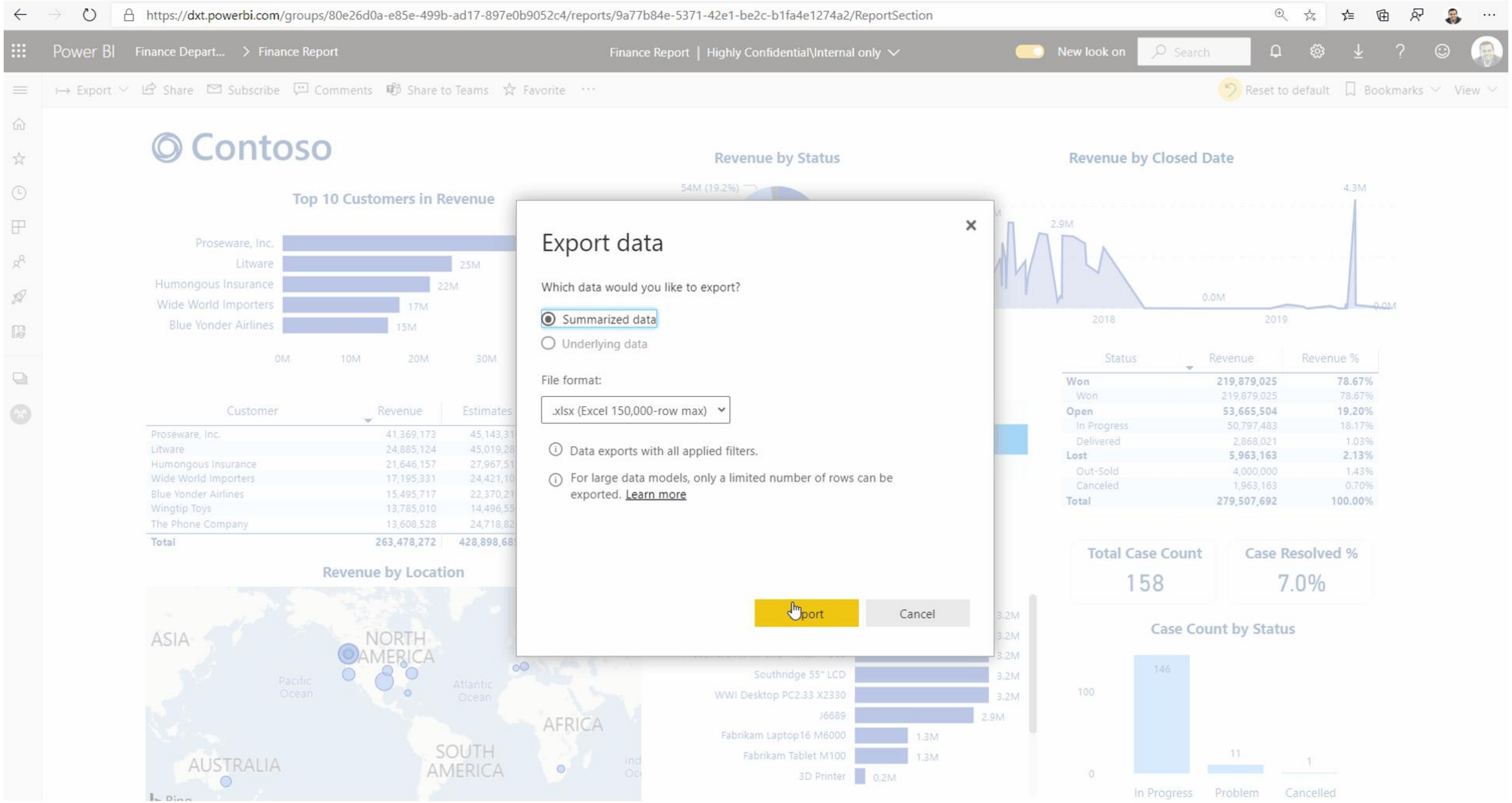
Customer	Revenue	Estimates	Variance
Proseware, Inc.	41,369,173	45,143,310.0	-3,774,137
Litware	24,885,124	45,019,281.0	-20,134,157
Humongous Insurance	21,646,157	27,967,513.0	-6,321,356
Wide World Importers	17,195,331	24,421,105.0	-7,225,774
Blue Yonder Airlines	15,495,717	22,370,217.0	-6,874,500
Wingtip Toys	13,785,010	14,496,556.0	-711,546
The Phone Company	13,608,528	24,718,826.0	-11,110,298
Total	**263,478,272**	**428,898,685.5**	**-165,420,413**

Status	Revenue	Revenue %
Won	**219,879,025**	**78.67%**
Won	219,879,025	78.67%
Open	**53,665,504**	**19.20%**
In Progress	50,797,483	18.17%
Delivered	2,868,021	1.03%
Lost	**5,963,163**	**2.13%**
Out-Sold	4,000,000	1.43%
Canceled	1,963,163	0.70%
Total	**279,507,692**	**100.00%**

Total Case Count
158

Case Resolved %
7.0%

Sensitivity labels and protection on exported data



Customer	Revenue	Estimates
Proseware, Inc.	41,369,173	45,143,31
Litware	24,885,124	45,019,28
Humongous Insurance	21,646,157	27,967,51
Wide World Importers	17,195,331	24,421,10
Blue Yonder Airlines	15,495,717	22,370,21
Wingtip Toys	13,785,010	14,496,55
The Phone Company	13,608,528	24,718,82
Total	**263,478,272**	**428,898,68**

Status	Revenue	Revenue %
Won	**219,879,025**	**78.67%**
Won	219,879,025	78.67%
Open	**53,665,504**	**19.20%**
In Progress	50,797,483	18.17%
Delivered	2,868,021	1.03%
Lost	**5,963,163**	**2.13%**
Out-Sold	4,000,000	1.43%
Canceled	1,963,163	0.70%
Total	**279,507,692**	**100.00%**

Total Case Count
158

Case Resolved %
7.0%

Export data

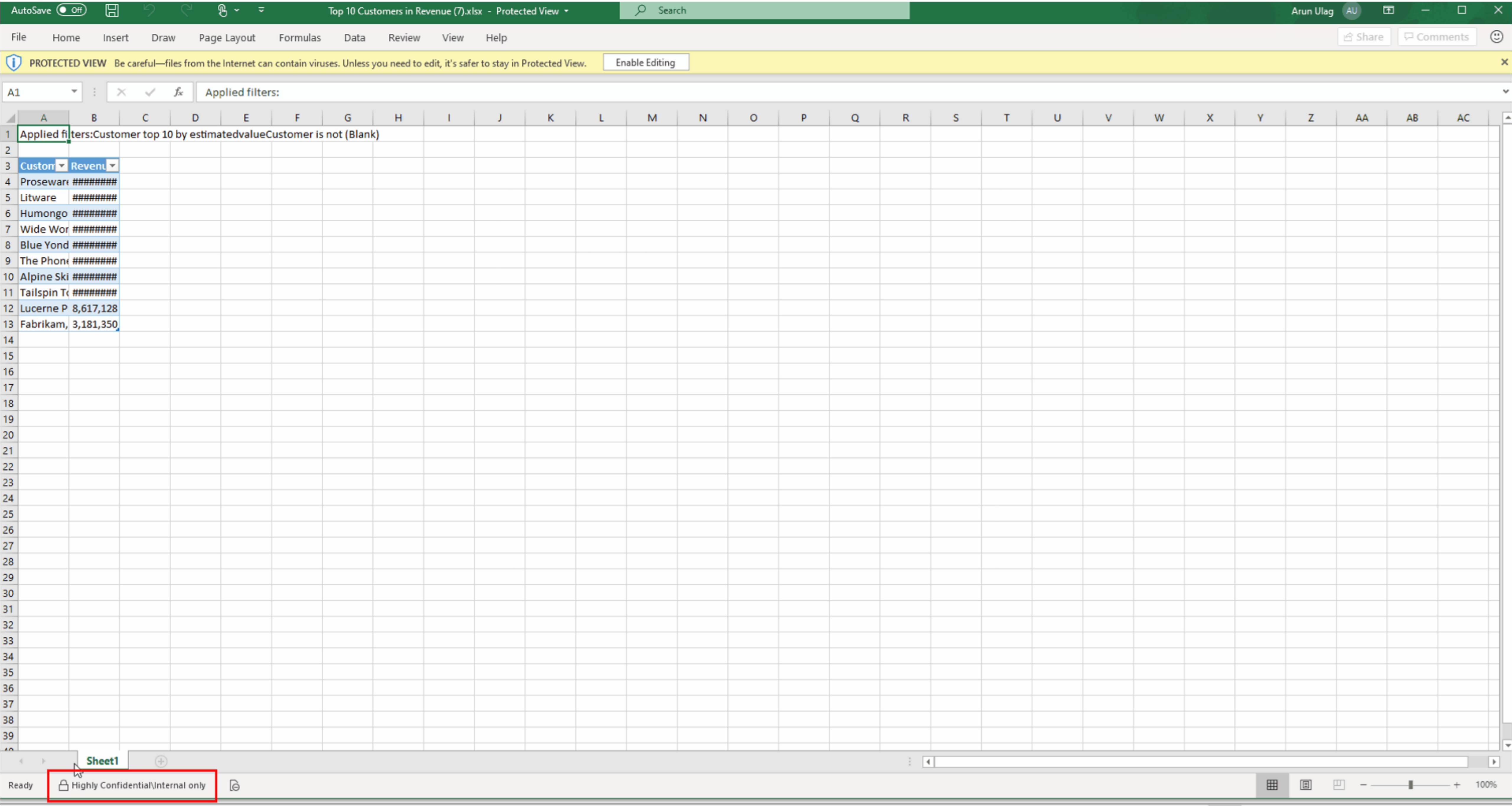
Which data would you like to export?

● Summarized data
○ Underlying data

File format:
.xlsx (Excel 150,000-row max)

ⓘ Data exports with all applied filters.

ⓘ For large data models, only a limited number of rows can be exported. Learn more



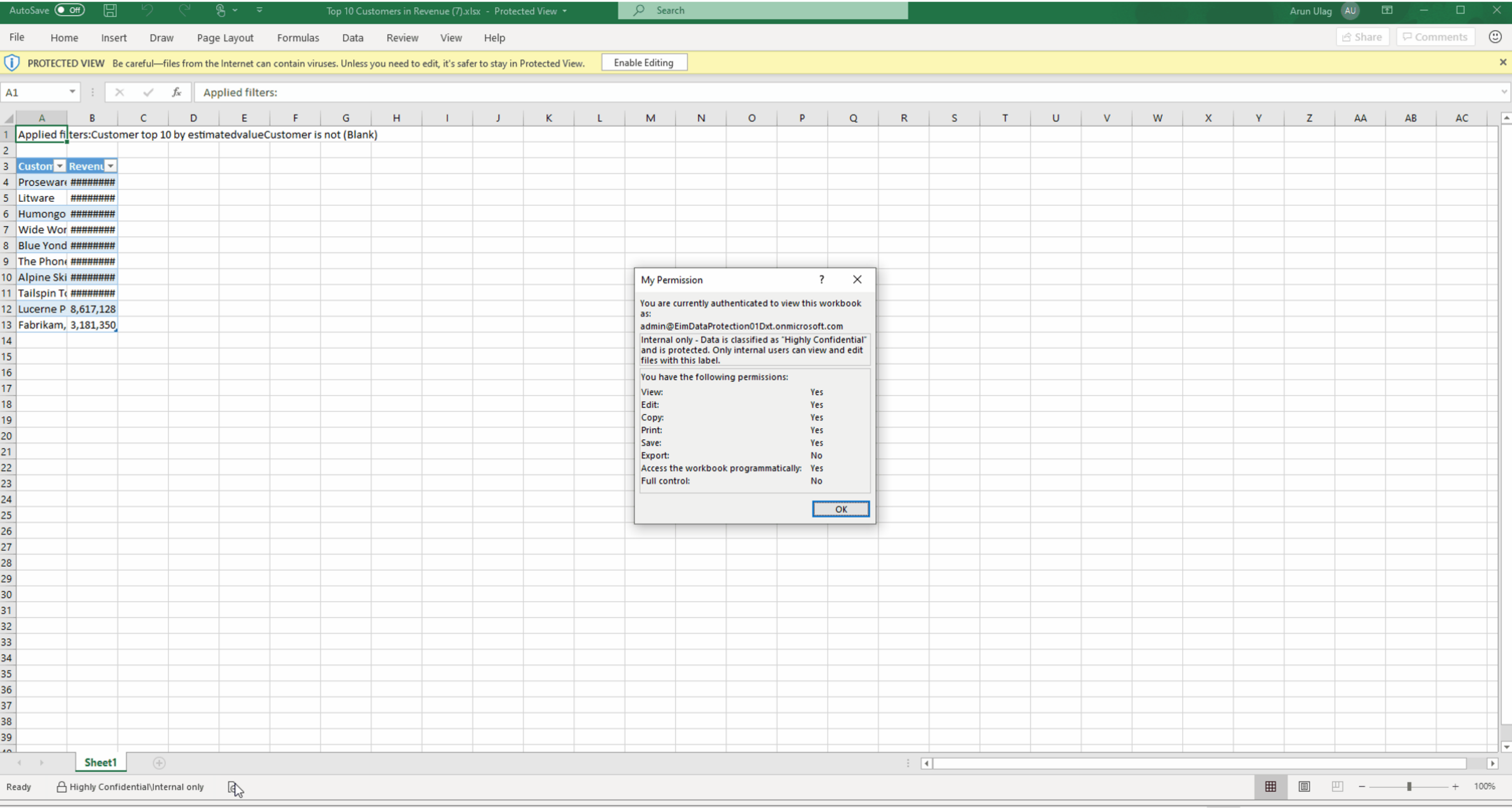
PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

Applied filters:

Applied filters:Customer top 10 by estimatedvalueCustomer is not (Blank)

Custom	Revenu
Proseware	########
Litware	########
Humongo	########
Wide Wor	########
Blue Yond	########
The Phone	########
Alpine Ski	########
Tailspin T	########
Lucerne P	8,617,128
Fabrikam,	3,181,350

Highly Confidential\Internal only



PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

Applied filters:

Applied filters:Customer top 10 by estimatedvalueCustomer is not (Blank)

Custon	Revenu
Prosewar	#########
Litware	#########
Humongo	#########
Wide Wor	#########
Blue Yond	#########
The Phon	#########
Alpine Ski	#########
Tailspin T	#########
Lucerne P	8,617,128
Fabrikam,	3,181,350

My Permission

You are currently authenticated to view this workbook as:
admin@EimDataProtection01Dxt.onmicrosoft.com

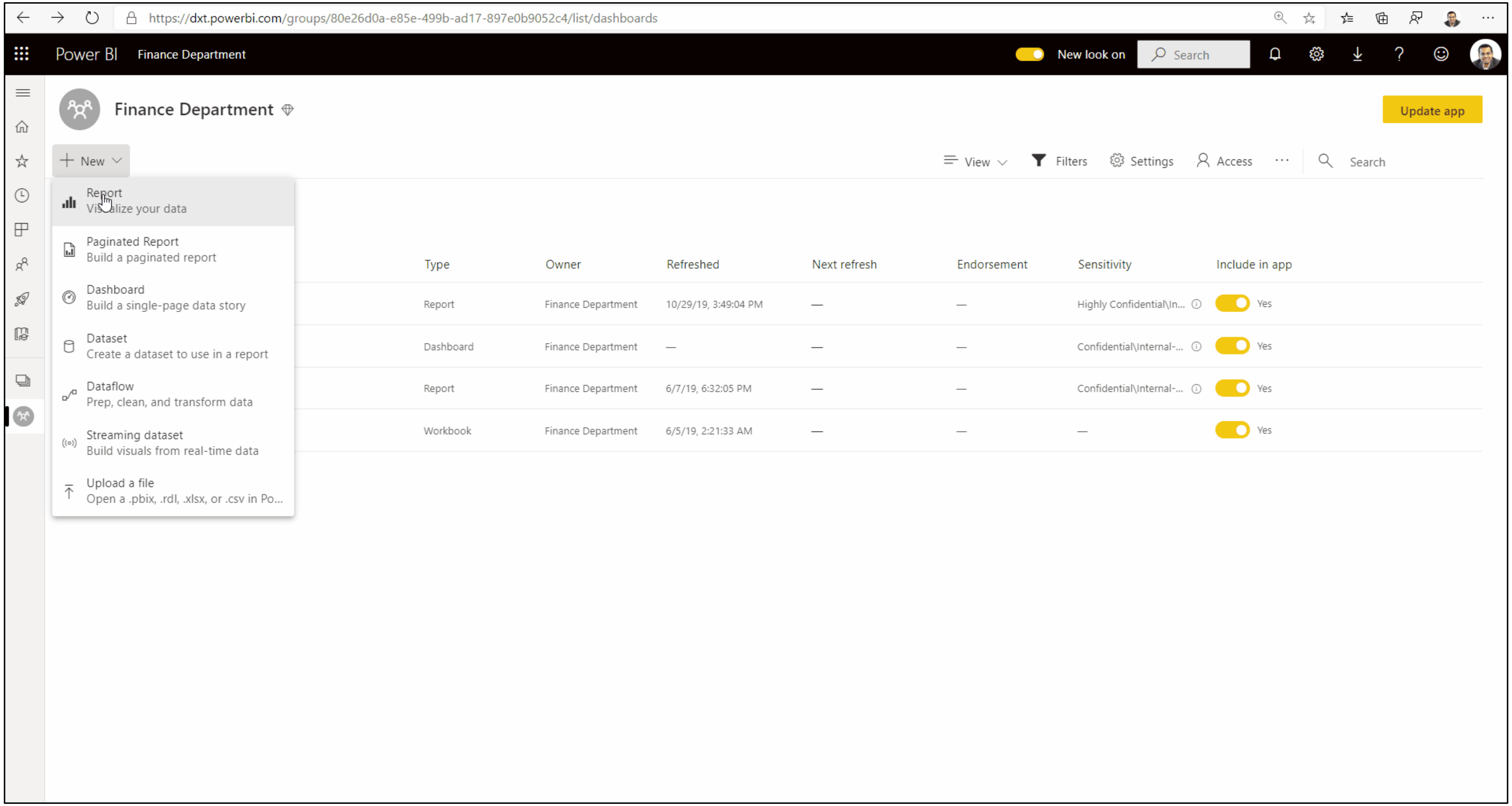
Internal only - Data is classified as "Highly Confidential" and is protected. Only internal users can view and edit files with this label.

You have the following permissions:

View:	Yes
Edit:	Yes
Copy:	Yes
Print:	Yes
Save:	Yes
Export:	No
Access the workbook programmatically:	Yes
Full control:	No

Highly Confidential\Internal only

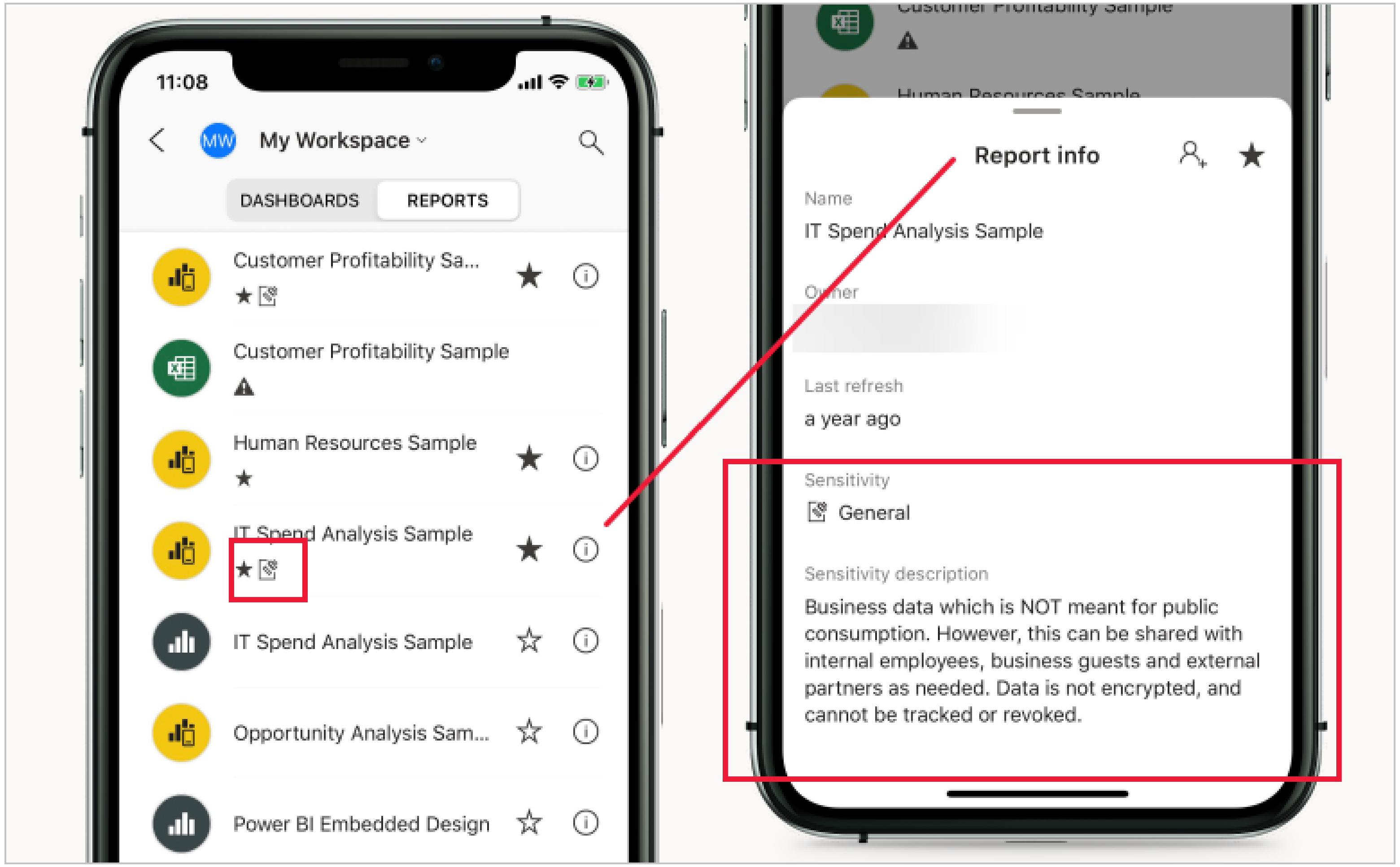
Sensitivity label inheritance upon creation of new content



https://dxt.powerbi.com/groups/80e26d0a-e85e-499b-ad17-897e0b9052c4/list/dashboards
Power BI
Finance Department
New look on
Search
Finance Department
Update app
New
View
Filters
Settings
Access
Search
Report
Visualize your data
Paginated Report
Build a paginated report
Dashboard
Build a single-page data story
Dataset
Create a dataset to use in a report
Dataflow
Prep, clean, and transform data
Streaming dataset
Build visuals from real-time data
Upload a file
Open a .pbix, .rdl, .xlsx, or .csv in Po...

Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Include in app
Report	Finance Department	10/29/19, 3:49:04 PM	—	—	Highly Confidential\In...	Yes
Dashboard	Finance Department	—	—	—	Confidential\Internal-...	Yes
Report	Finance Department	6/7/19, 6:32:05 PM	—	—	Confidential\Internal-...	Yes
Workbook	Finance Department	6/5/19, 2:21:33 AM	—	—	—	Yes

Sensitivity labels in the Power BI mobile apps



Report info

Name

IT Spend Analysis Sample

Owner

[redacted]

Last refresh

a year ago

Sensitivity

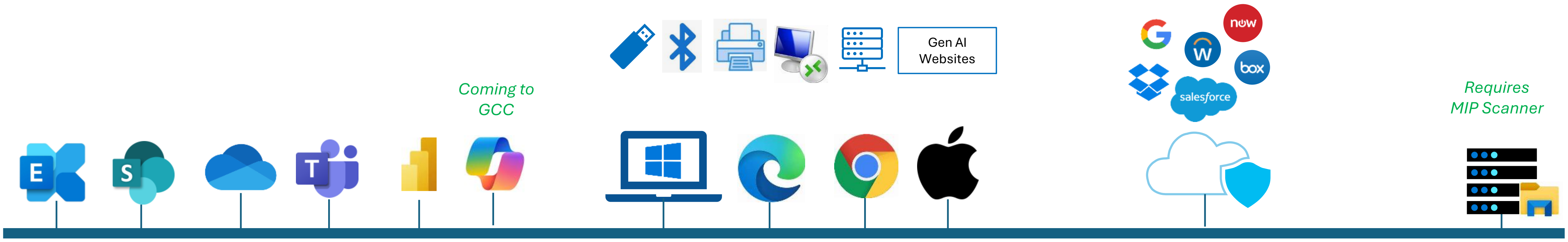
General

Sensitivity description

Business data which is NOT meant for public consumption. However, this can be shared with internal employees, business guests and external partners as needed. Data is not encrypted, and cannot be tracked or revoked.

Microsoft Purview Data Loss Prevention

Prevent accidental or unauthorized sharing of sensitive data



Coming to GCC

Requires MIP Scanner

Microsoft 365
Cloud DLP – Service based

Endpoint
Endpoint – Platform based

Non-Microsoft apps
3rd party API based

On-premises
On-prem service

Data in use

Data in motion

Data at rest

Guided onboarding

Unified & flexible policy management

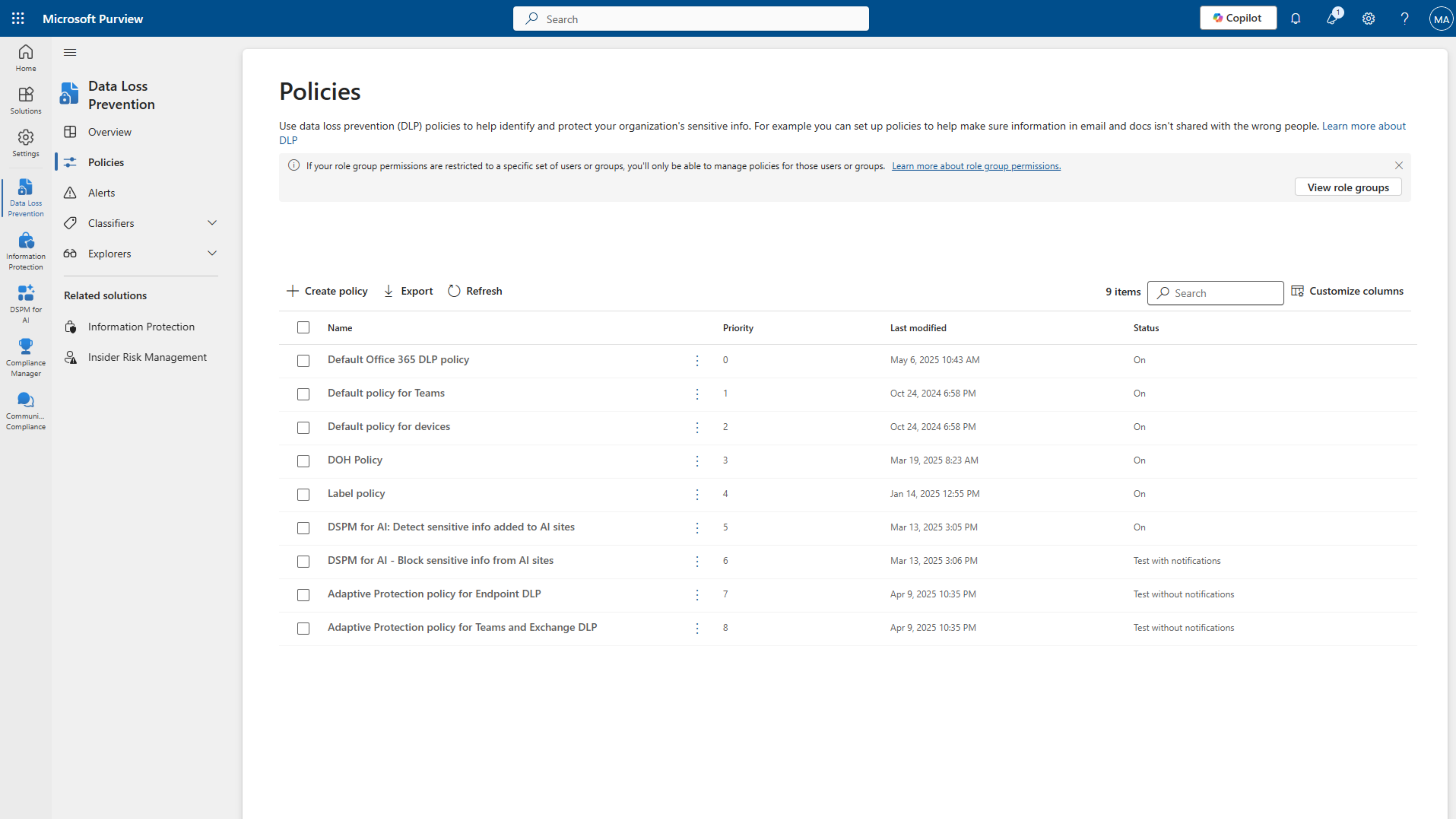
Integrated with Microsoft Purview Information Protection

Unified alerting & remediation

Agentless and integrated within end user experiences

DLP – Admin Experience

- DLP Policy Creation

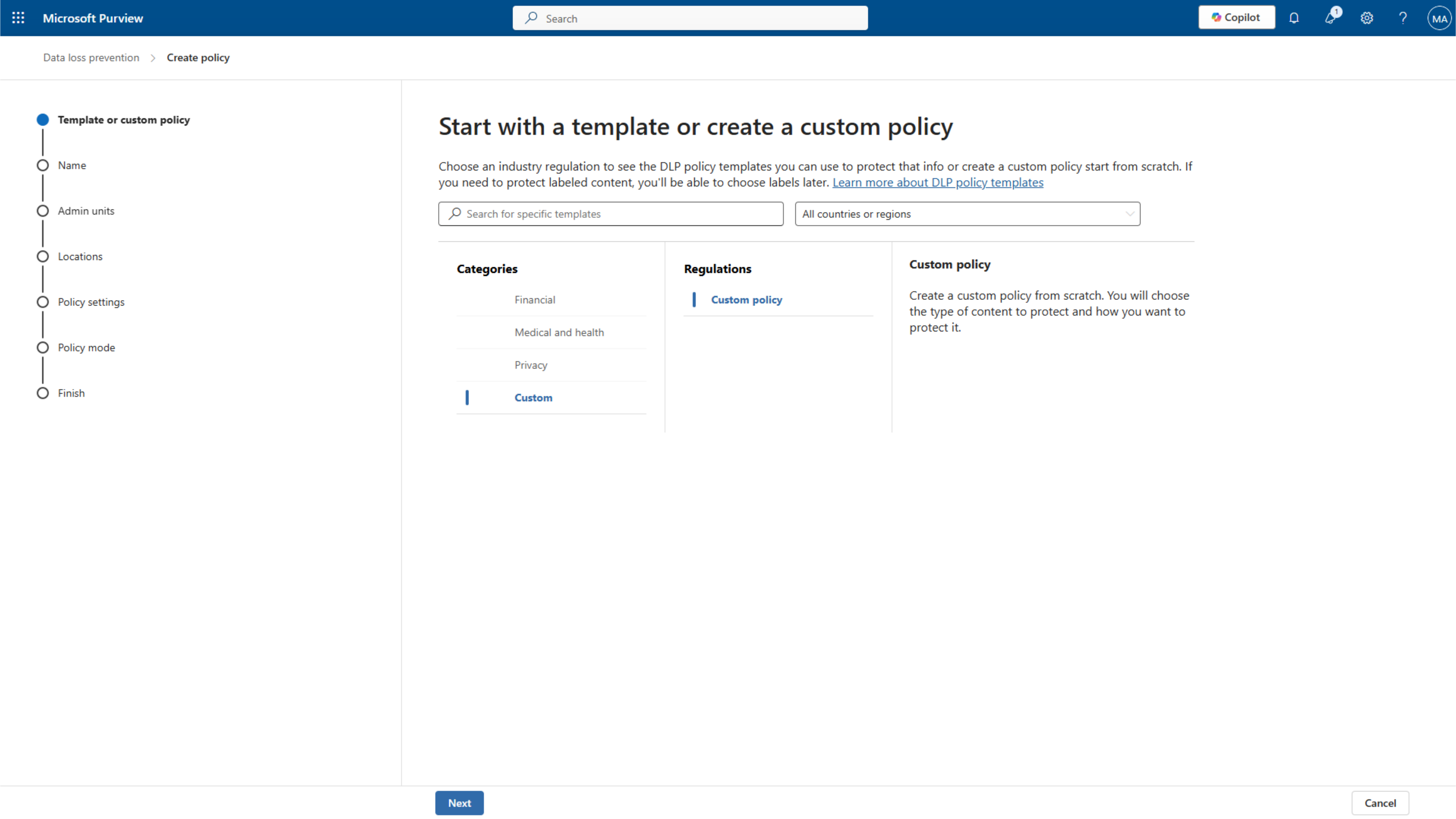


Policies

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. Learn more about DLP

ⓘ If your role group permissions are restricted to a specific set of users or groups, you'll only be able to manage policies for those users or groups. Learn more about role group permissions.

Name	Priority	Last modified	Status
Default Office 365 DLP policy	0	May 6, 2025 10:43 AM	On
Default policy for Teams	1	Oct 24, 2024 6:58 PM	On
Default policy for devices	2	Oct 24, 2024 6:58 PM	On
DOH Policy	3	Mar 19, 2025 8:23 AM	On
Label policy	4	Jan 14, 2025 12:55 PM	On
DSPM for AI: Detect sensitive info added to AI sites	5	Mar 13, 2025 3:05 PM	On
DSPM for AI - Block sensitive info from AI sites	6	Mar 13, 2025 3:06 PM	Test with notifications
Adaptive Protection policy for Endpoint DLP	7	Apr 9, 2025 10:35 PM	Test without notifications
Adaptive Protection policy for Teams and Exchange DLP	8	Apr 9, 2025 10:35 PM	Test without notifications



Start with a template or create a custom policy

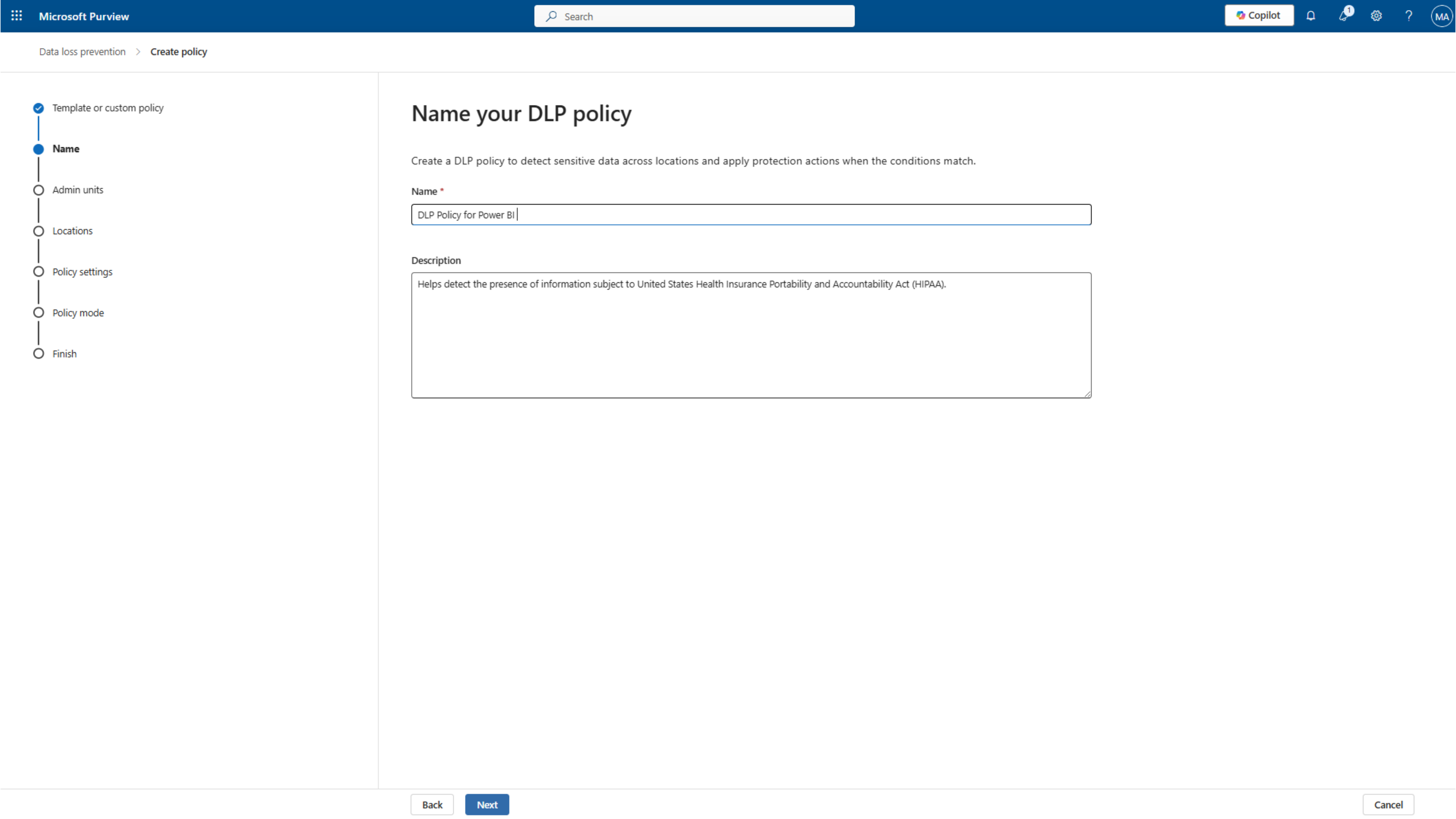
Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. Learn more about DLP policy templates

Categories: Custom

Regulations: Custom policy

Custom policy

Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.



Name your DLP policy

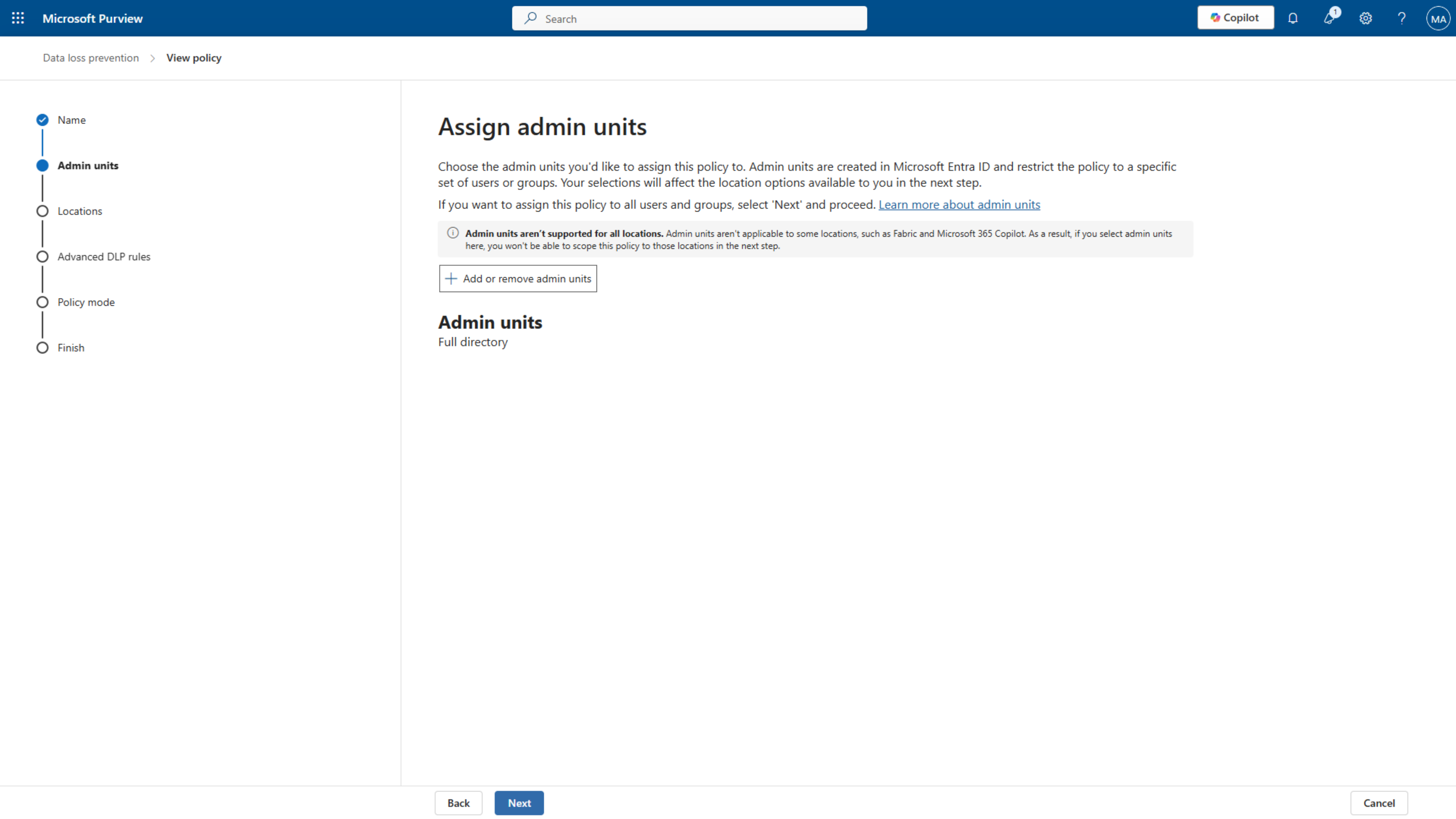
Create a DLP policy to detect sensitive data across locations and apply protection actions when the conditions match.

Name *

DLP Policy for Power BI

Description

Helps detect the presence of information subject to United States Health Insurance Portability and Accountability Act (HIPAA).



Assign admin units

Choose the admin units you'd like to assign this policy to. Admin units are created in Microsoft Entra ID and restrict the policy to a specific set of users or groups. Your selections will affect the location options available to you in the next step.

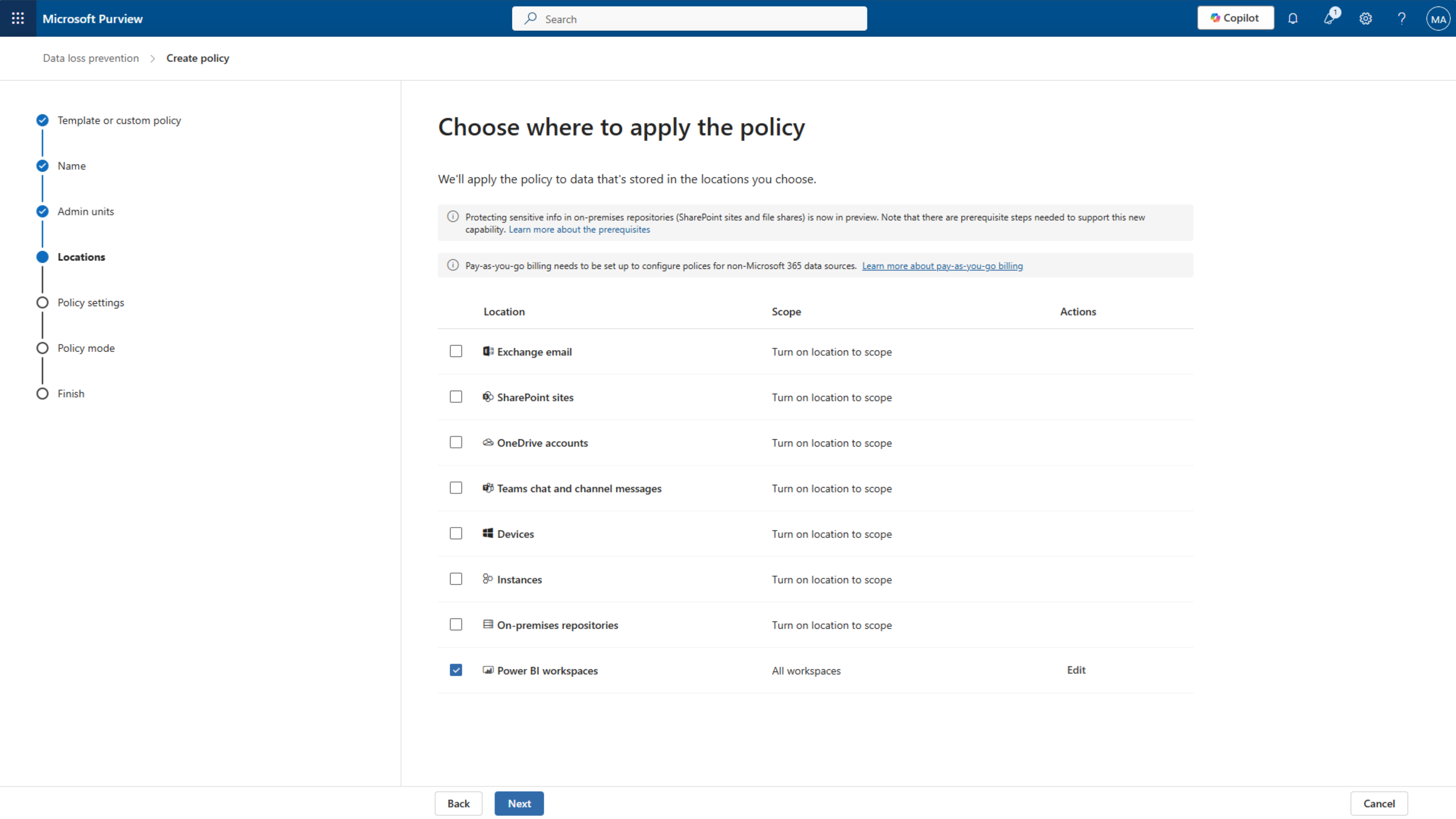
If you want to assign this policy to all users and groups, select 'Next' and proceed. Learn more about admin units

Admin units aren't supported for all locations. Admin units aren't applicable to some locations, such as Fabric and Microsoft 365 Copilot. As a result, if you select admin units here, you won't be able to scope this policy to those locations in the next step.

+ Add or remove admin units

Admin units

Full directory



Data loss prevention > **Create policy**

- ● Template or custom policy
- ● Name
- ● Admin units
- ● **Locations**
- ○ Policy settings
- ○ Policy mode
- ○ Finish

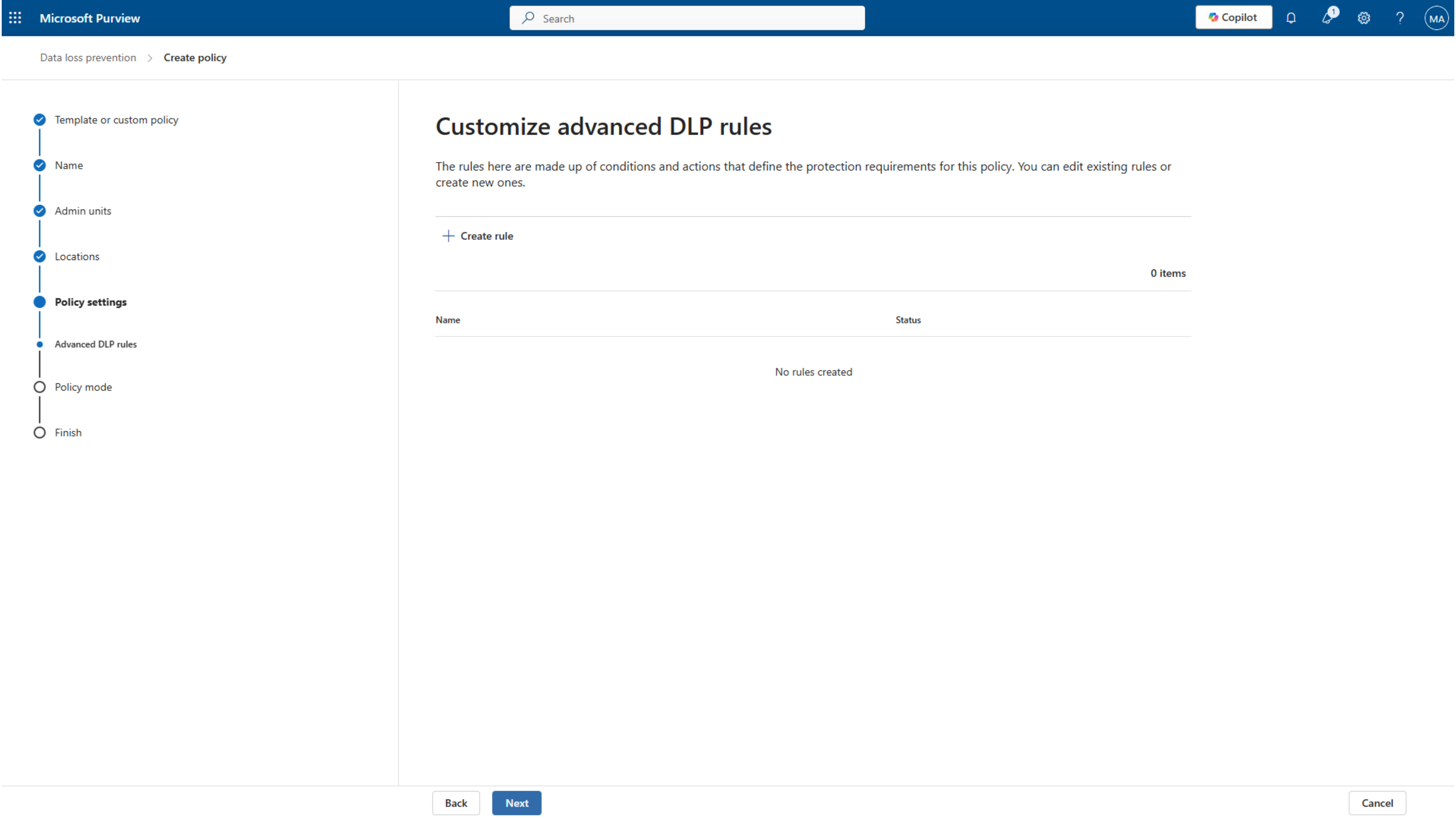
Choose where to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

ⓘ Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. Learn more about the prerequisites

ⓘ Pay-as-you-go billing needs to be set up to configure polices for non-Microsoft 365 data sources. Learn more about pay-as-you-go billing

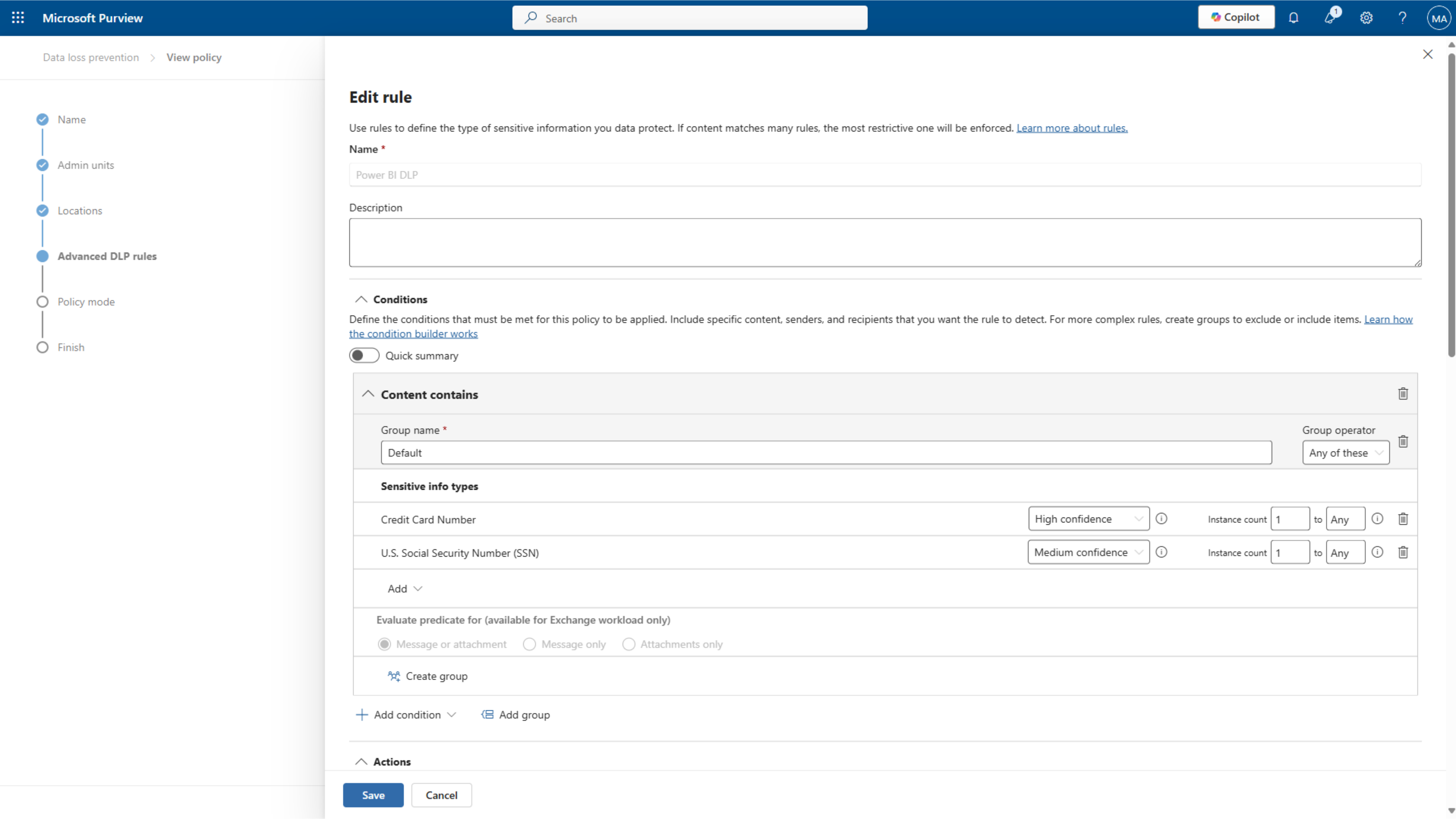
	Location	Scope	Actions
☐	**Exchange email**	Turn on location to scope	
☐	**SharePoint sites**	Turn on location to scope	
☐	**OneDrive accounts**	Turn on location to scope	
☐	**Teams chat and channel messages**	Turn on location to scope	
☐	**Devices**	Turn on location to scope	
☐	**Instances**	Turn on location to scope	
☐	**On-premises repositories**	Turn on location to scope	
☑	**Power BI workspaces**	All workspaces	Edit



Customize advanced DLP rules

The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones.

Name	Status
No rules created	



Edit rule

Use rules to define the type of sensitive information you data protect. If content matches many rules, the most restrictive one will be enforced. Learn more about rules.

Name *

Power BI DLP

Description

Conditions

Define the conditions that must be met for this policy to be applied. Include specific content, senders, and recipients that you want the rule to detect. For more complex rules, create groups to exclude or include items. Learn how the condition builder works

○ Quick summary

Content contains

Group name *: Default

Group operator: Any of these

Sensitive info types

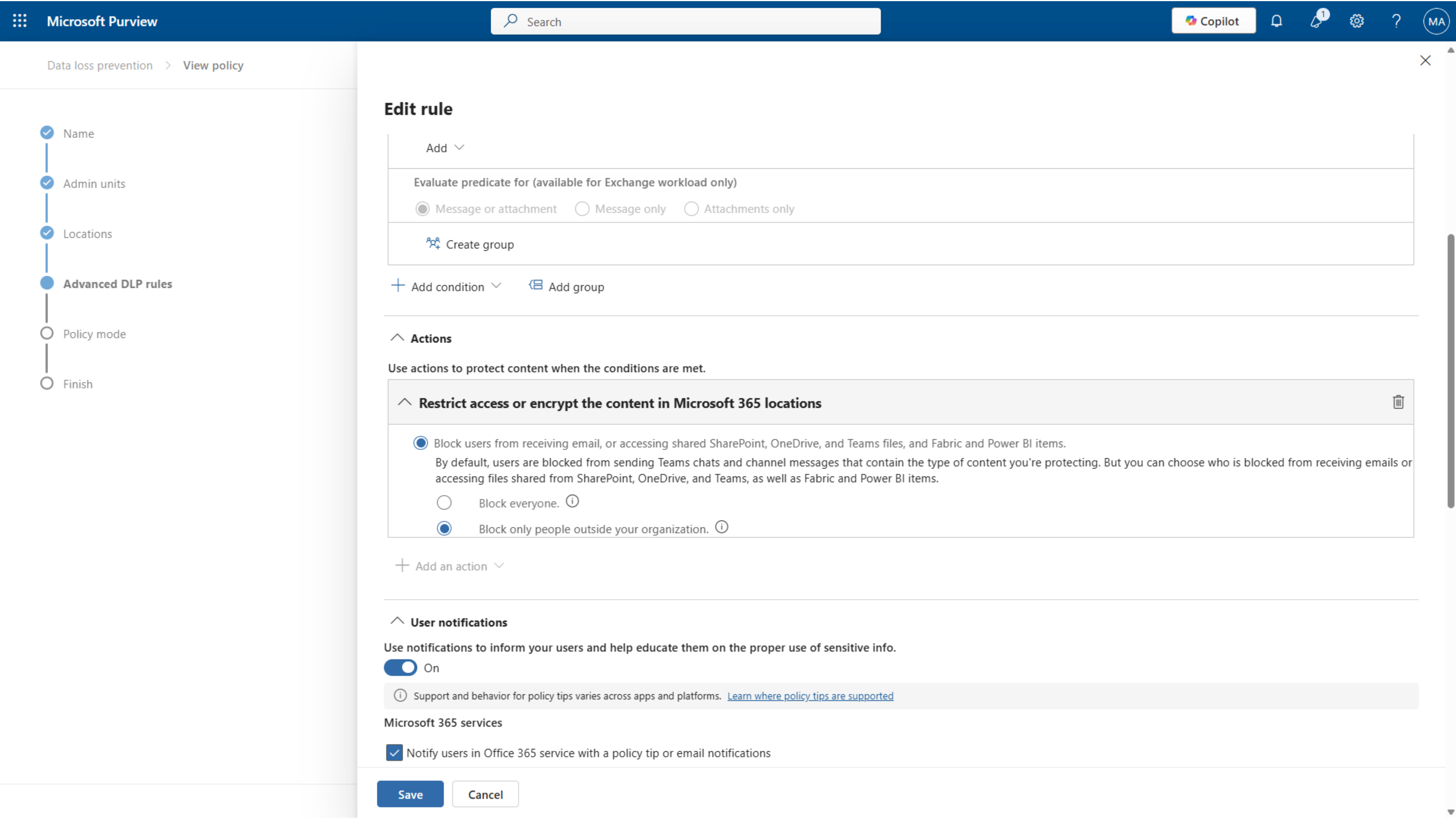
Credit Card Number	High confidence	Instance count 1	to Any
U.S. Social Security Number (SSN)	Medium confidence	Instance count 1	to Any

Add

Evaluate predicate for (available for Exchange workload only)

● Message or attachment ○ Message only ○ Attachments only

Actions



Edit rule

Add

Evaluate predicate for (available for Exchange workload only)

● Message or attachment ○ Message only ○ Attachments only

Create group

+ Add condition   Add group

Actions

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content in Microsoft 365 locations

● Block users from receiving email, or accessing shared SharePoint, OneDrive, and Teams files, and Fabric and Power BI items.

By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams, as well as Fabric and Power BI items.

○ Block everyone.

● Block only people outside your organization.

+ Add an action

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

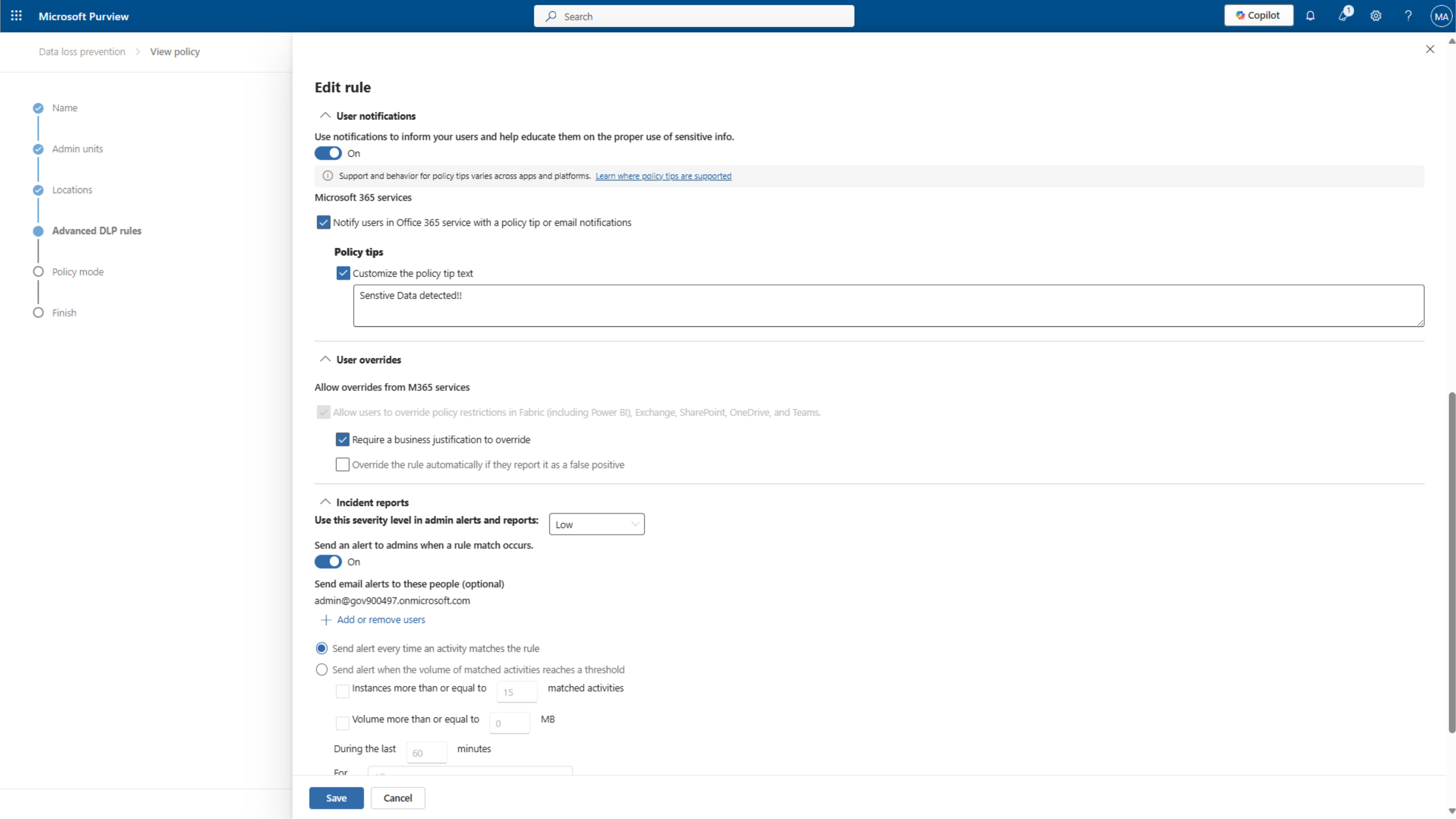
On

Support and behavior for policy tips varies across apps and platforms. Learn where policy tips are supported

Microsoft 365 services

☑ Notify users in Office 365 service with a policy tip or email notifications

Save   Cancel



Edit rule

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

On

Support and behavior for policy tips varies across apps and platforms. Learn where policy tips are supported

Microsoft 365 services

☑ Notify users in Office 365 service with a policy tip or email notifications

Policy tips

☑ Customize the policy tip text

Senstive Data detected!!

User overrides

Allow overrides from M365 services

☑ Allow users to override policy restrictions in Fabric (including Power BI), Exchange, SharePoint, OneDrive, and Teams.

☑ Require a business justification to override

□ Override the rule automatically if they report it as a false positive

Incident reports

Use this severity level in admin alerts and reports: Low

Send an alert to admins when a rule match occurs.

On

Send email alerts to these people (optional)

admin@gov900497.onmicrosoft.com

+ Add or remove users

● Send alert every time an activity matches the rule

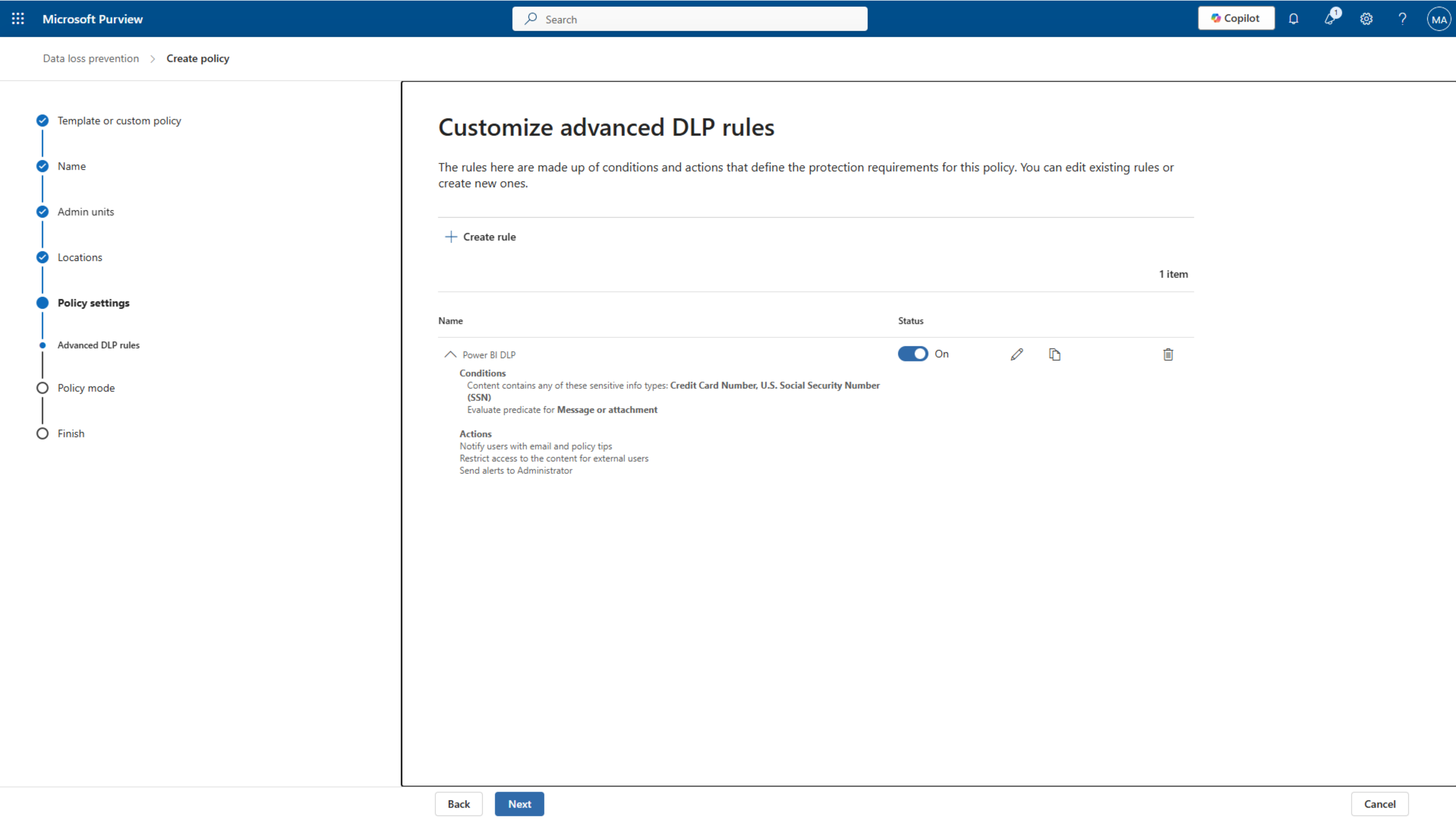
○ Send alert when the volume of matched activities reaches a threshold

□ Instances more than or equal to 15 matched activities

□ Volume more than or equal to 0 MB

During the last 60 minutes

For



Customize advanced DLP rules

The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones.

1 item

Name	Status
Power BI DLP	On

Conditions

Content contains any of these sensitive info types: **Credit Card Number, U.S. Social Security Number (SSN)**

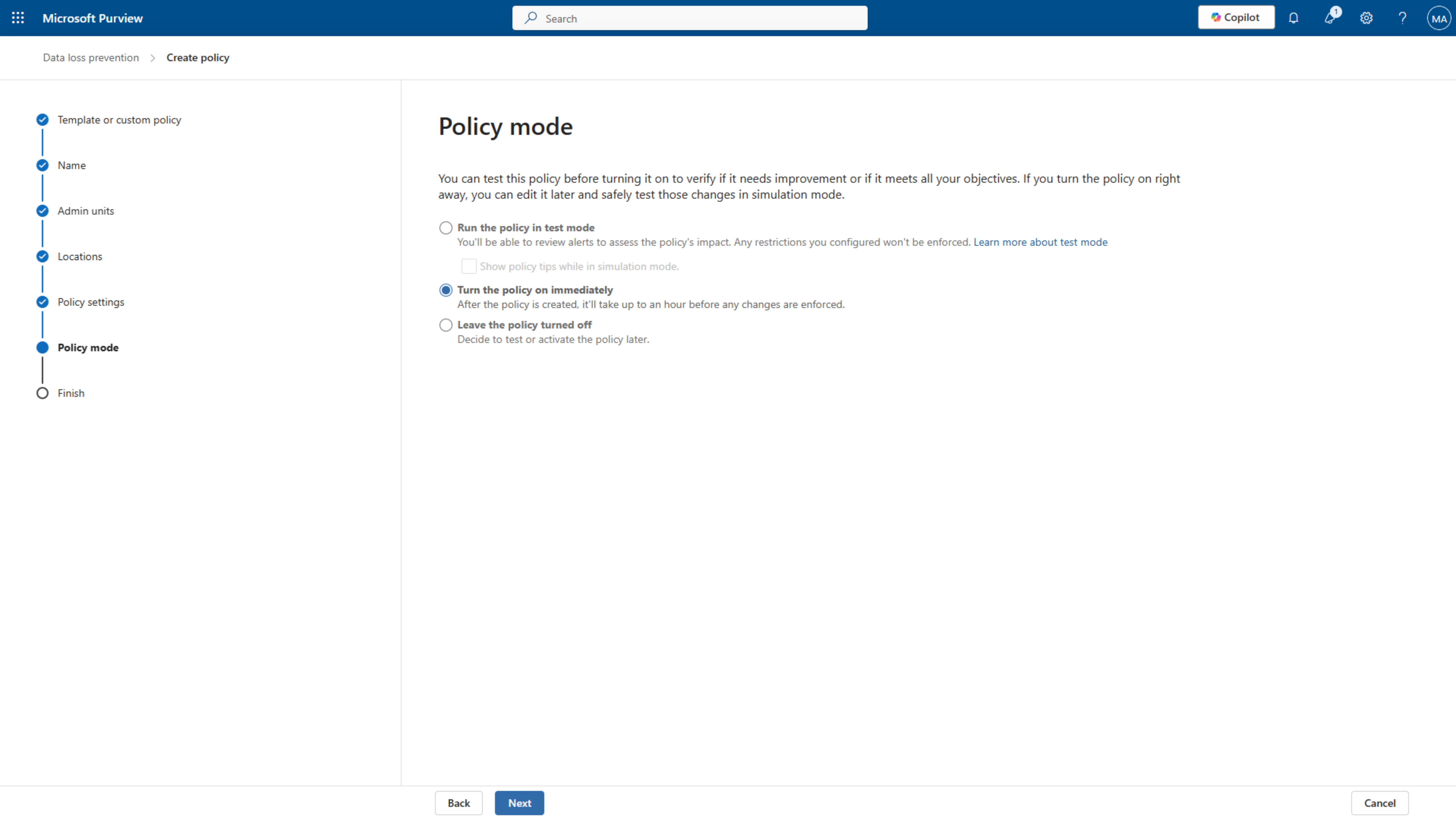
Evaluate predicate for **Message or attachment**

Actions

Notify users with email and policy tips

Restrict access to the content for external users

Send alerts to Administrator



Policy mode

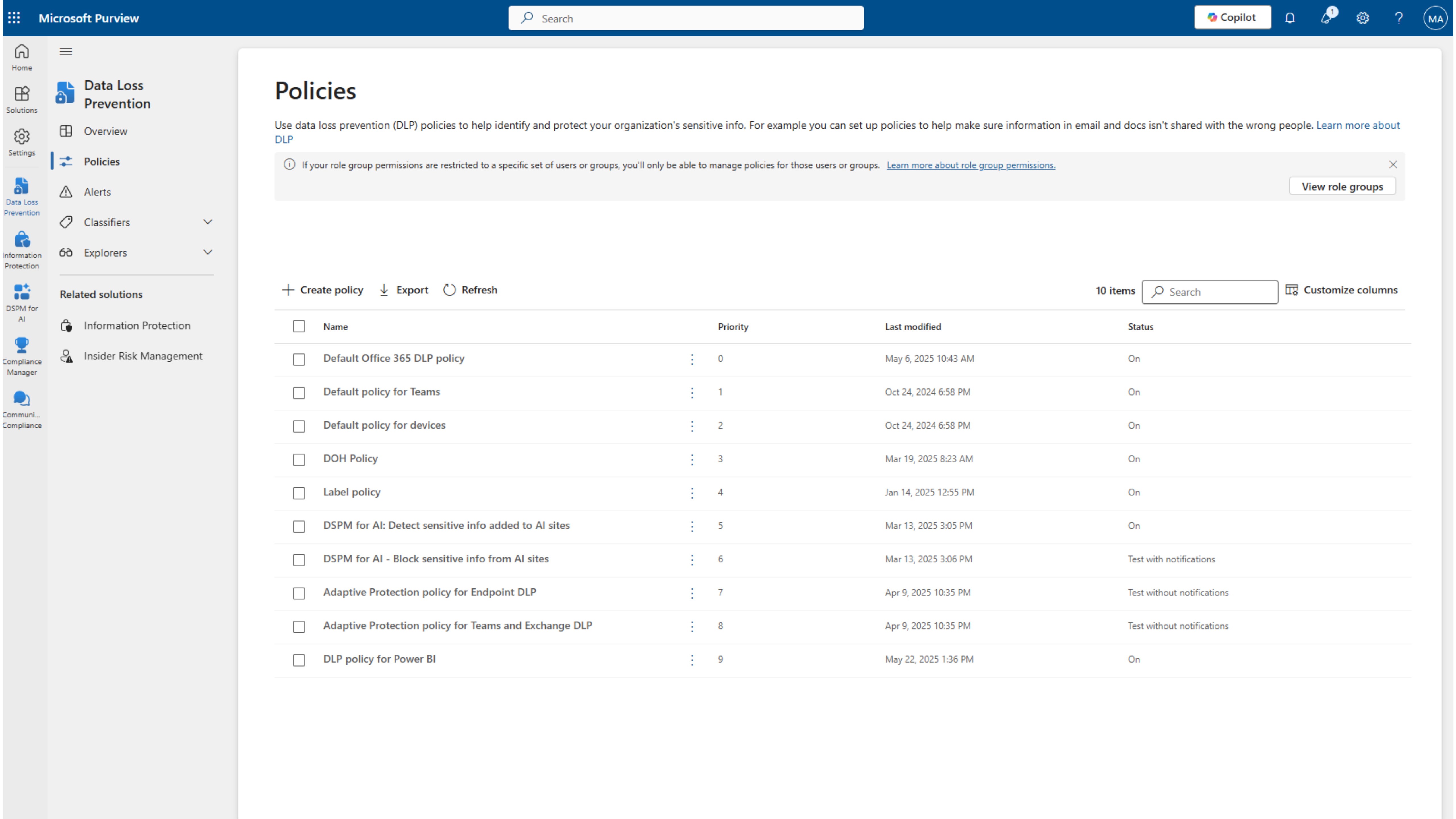
You can test this policy before turning it on to verify if it needs improvement or if it meets all your objectives. If you turn the policy on right away, you can edit it later and safely test those changes in simulation mode.

○ **Run the policy in test mode**
You'll be able to review alerts to assess the policy's impact. Any restrictions you configured won't be enforced. Learn more about test mode

□ Show policy tips while in simulation mode.

● **Turn the policy on immediately**
After the policy is created, it'll take up to an hour before any changes are enforced.

○ **Leave the policy turned off**
Decide to test or activate the policy later.



Policies

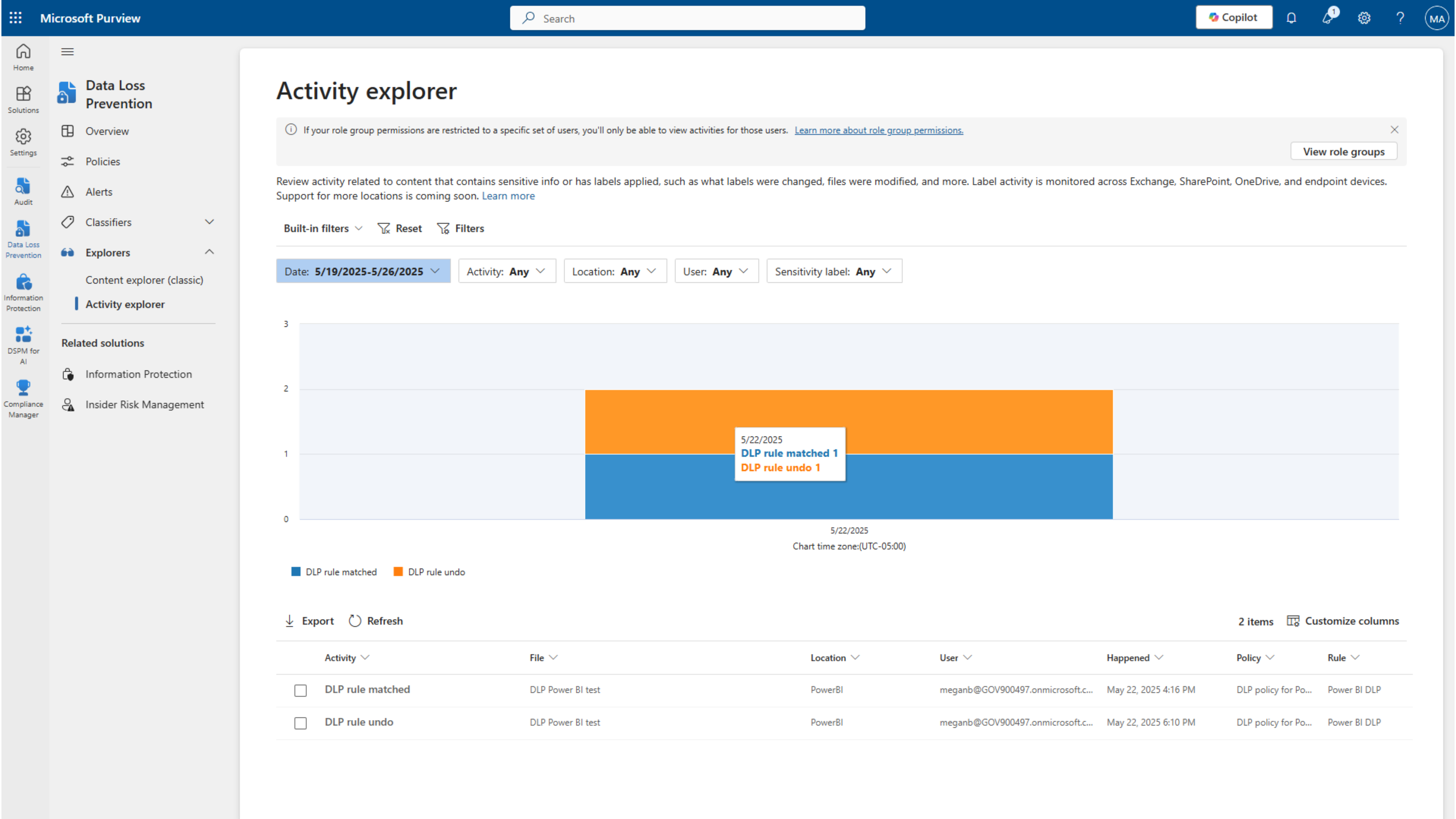
Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. Learn more about DLP

ⓘ If your role group permissions are restricted to a specific set of users or groups, you'll only be able to manage policies for those users or groups. Learn more about role group permissions.

□	Name	Priority	Last modified	Status
□	Default Office 365 DLP policy	0	May 6, 2025 10:43 AM	On
□	Default policy for Teams	1	Oct 24, 2024 6:58 PM	On
□	Default policy for devices	2	Oct 24, 2024 6:58 PM	On
□	DOH Policy	3	Mar 19, 2025 8:23 AM	On
□	Label policy	4	Jan 14, 2025 12:55 PM	On
□	DSPM for AI: Detect sensitive info added to AI sites	5	Mar 13, 2025 3:05 PM	On
□	DSPM for AI - Block sensitive info from AI sites	6	Mar 13, 2025 3:06 PM	Test with notifications
□	Adaptive Protection policy for Endpoint DLP	7	Apr 9, 2025 10:35 PM	Test without notifications
□	Adaptive Protection policy for Teams and Exchange DLP	8	Apr 9, 2025 10:35 PM	Test without notifications
□	DLP policy for Power BI	9	May 22, 2025 1:36 PM	On

DLP – Admin Experience

- DLP Policy Matches



Data Loss Prevention

- Overview
- Policies
- Alerts
- Classifiers
- Explorers
  - Content explorer (classic)
  - Activity explorer

Related solutions

- Information Protection
- Insider Risk Management

Activity explorer

ⓘ If your role group permissions are restricted to a specific set of users, you'll only be able to view activities for those users. Learn more about role group permissions.

View role groups

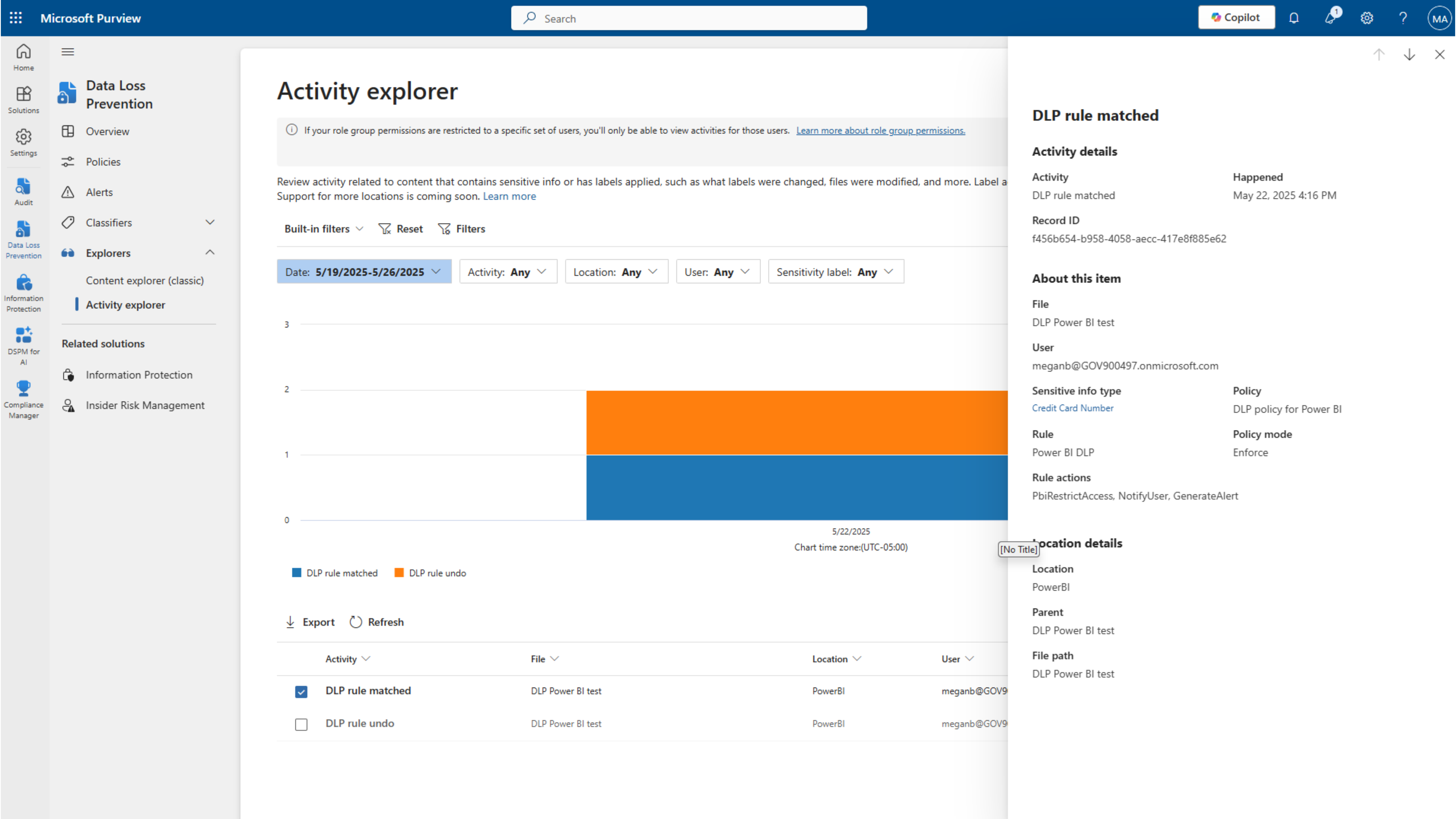
Review activity related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and more. Label activity is monitored across Exchange, SharePoint, OneDrive, and endpoint devices. Support for more locations is coming soon. Learn more

Built-in filters | Reset | Filters

Date: **5/19/2025-5/26/2025** | Activity: **Any** | Location: **Any** | User: **Any** | Sensitivity label: **Any**

Export | Refresh | 2 items | Customize columns

	Activity	File	Location	User	Happened	Policy	Rule
□	DLP rule matched	DLP Power BI test	PowerBI	meganb@GOV900497.onmicrosoft.c...	May 22, 2025 4:16 PM	DLP policy for Po...	Power BI DLP
□	DLP rule undo	DLP Power BI test	PowerBI	meganb@GOV900497.onmicrosoft.c...	May 22, 2025 6:10 PM	DLP policy for Po...	Power BI DLP



Activity explorer

ⓘ If your role group permissions are restricted to a specific set of users, you'll only be able to view activities for those users. Learn more about role group permissions.

Review activity related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and more. Label a
Support for more locations is coming soon. Learn more

Date: **5/19/2025-5/26/2025** | Activity: **Any** | Location: **Any** | User: **Any** | Sensitivity label: **Any**

■ DLP rule matched ■ DLP rule undo

	Activity	File	Location	User
☑	DLP rule matched	DLP Power BI test	PowerBI	meganb@GOV9
□	DLP rule undo	DLP Power BI test	PowerBI	meganb@GOV9

DLP rule matched

Activity details

Activity
DLP rule matched

Happened
May 22, 2025 4:16 PM

Record ID
f456b654-b958-4058-aecc-417e8f885e62

About this item

File
DLP Power BI test

User
meganb@GOV900497.onmicrosoft.com

Sensitive info type
Credit Card Number

Policy
DLP policy for Power BI

Rule
Power BI DLP

Policy mode
Enforce

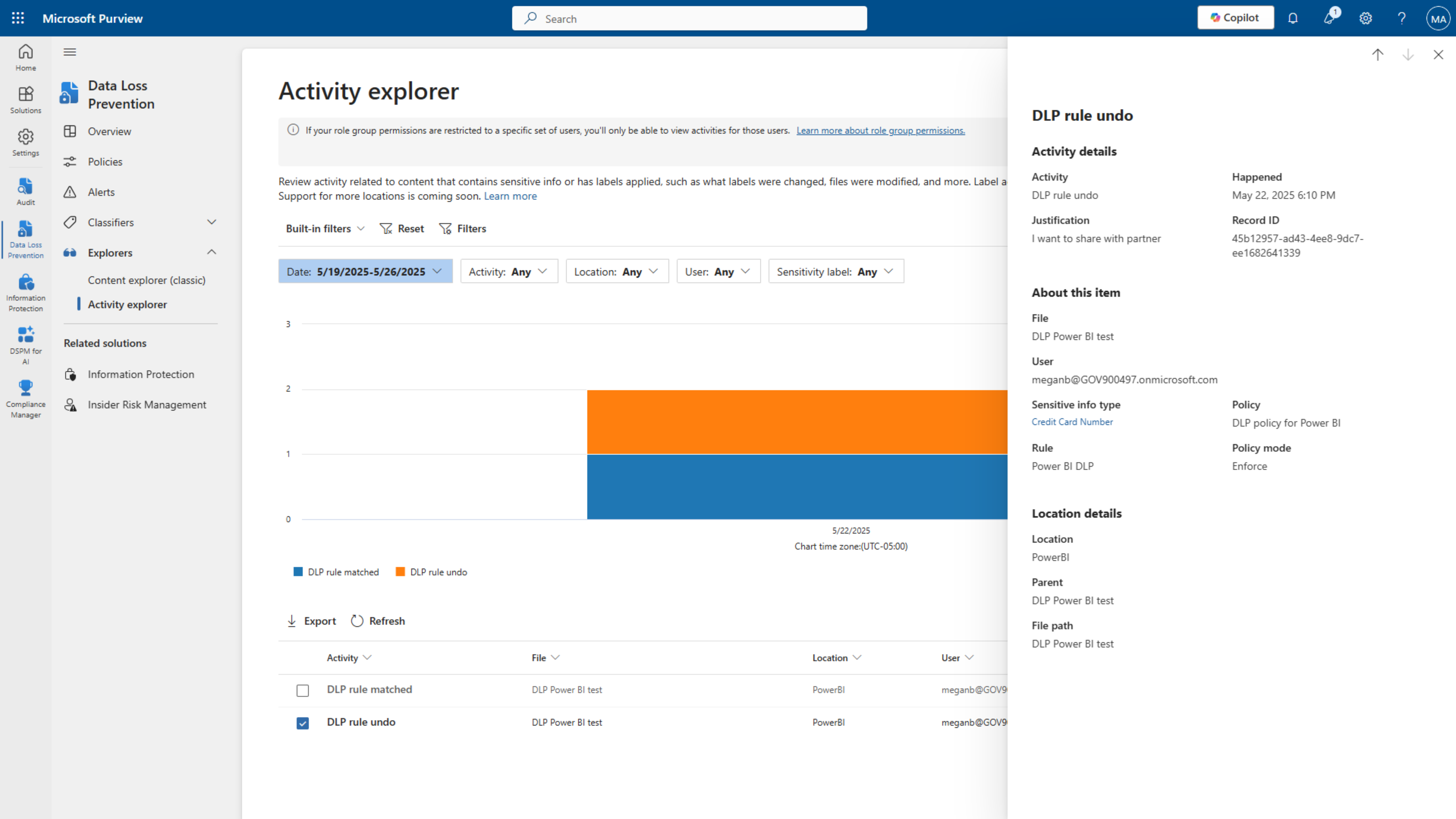
Rule actions
PbiRestrictAccess, NotifyUser, GenerateAlert

Location details

Location
PowerBI

Parent
DLP Power BI test

File path
DLP Power BI test



Data Loss Prevention

Activity explorer

ⓘ If your role group permissions are restricted to a specific set of users, you'll only be able to view activities for those users. Learn more about role group permissions.

Review activity related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and more. Label a
Support for more locations is coming soon. Learn more

Date: **5/19/2025-5/26/2025** | Activity: **Any** | Location: **Any** | User: **Any** | Sensitivity label: **Any**

	Activity	File	Location	User
☐	DLP rule matched	DLP Power BI test	PowerBI	meganb@GOV9
☑	**DLP rule undo**	DLP Power BI test	PowerBI	meganb@GOV9

DLP rule undo

Activity details

Activity
DLP rule undo

Happened
May 22, 2025 6:10 PM

Justification
I want to share with partner

Record ID
45b12957-ad43-4ee8-9dc7-ee1682641339

About this item

File
DLP Power BI test

User
meganb@GOV900497.onmicrosoft.com

Sensitive info type
Credit Card Number

Policy
DLP policy for Power BI

Rule
Power BI DLP

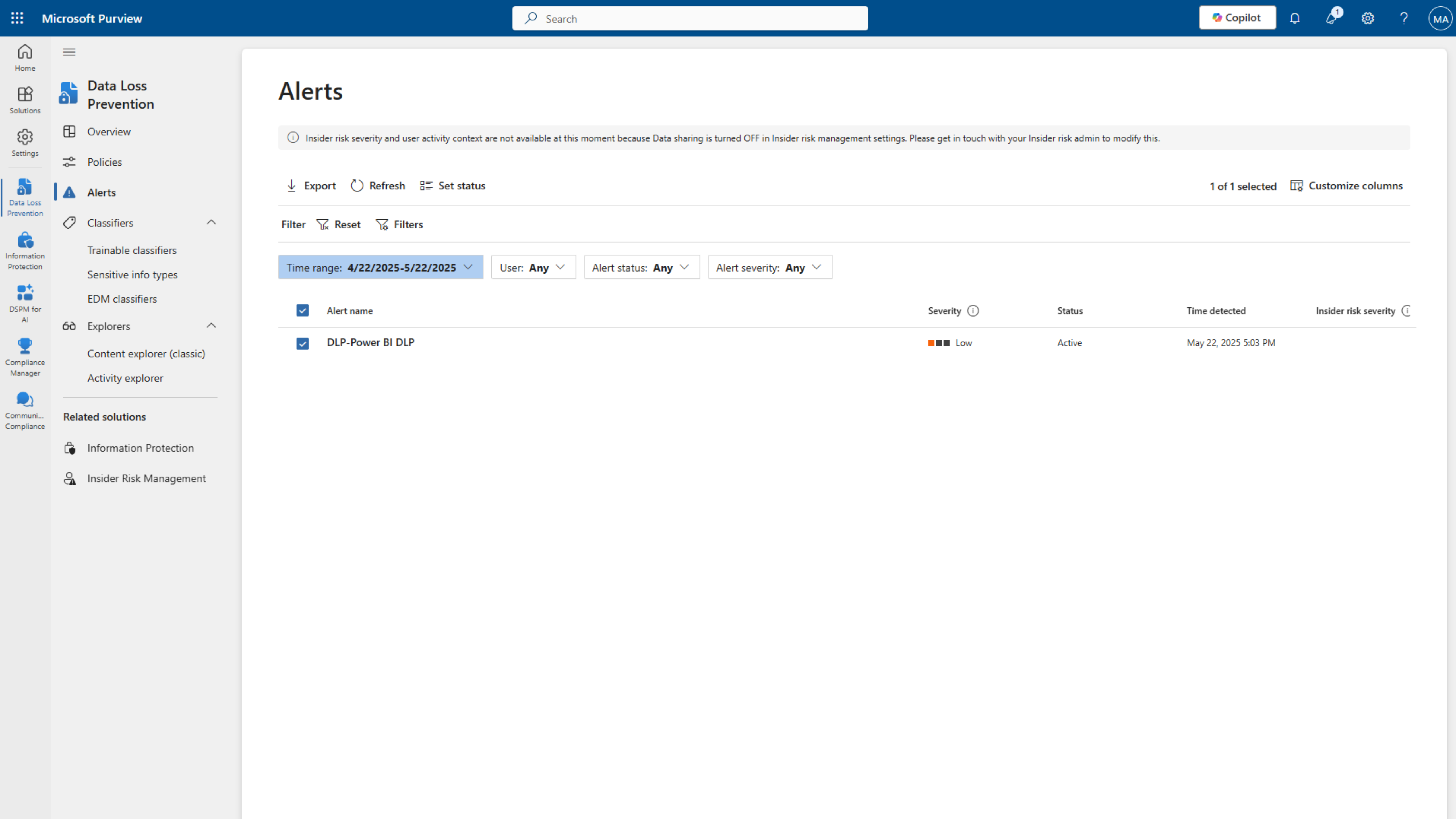
Policy mode
Enforce

Location details

Location
PowerBI

Parent
DLP Power BI test

File path
DLP Power BI test

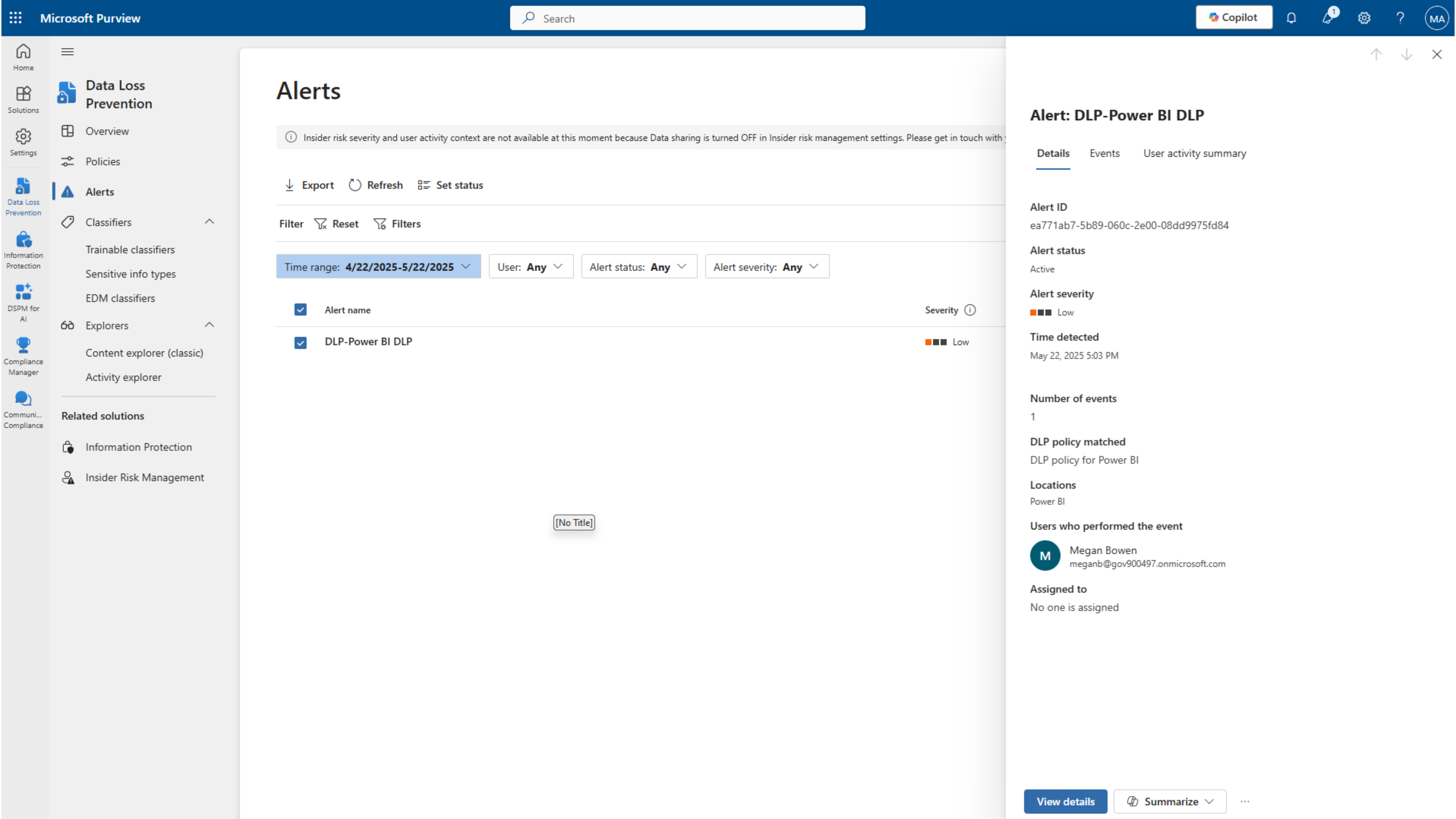


Alerts

Insider risk severity and user activity context are not available at this moment because Data sharing is turned OFF in Insider risk management settings. Please get in touch with your Insider risk admin to modify this.

Time range: 4/22/2025-5/22/2025 | User: Any | Alert status: Any | Alert severity: Any

☑	Alert name	Severity	Status	Time detected	Insider risk severity
☑	DLP-Power BI DLP	Low	Active	May 22, 2025 5:03 PM	



Alerts

ⓘ Insider risk severity and user activity context are not available at this moment because Data sharing is turned OFF in Insider risk management settings. Please get in touch with

Time range: **4/22/2025-5/22/2025** User: **Any** Alert status: **Any** Alert severity: **Any**

☑	Alert name	Severity
☑	DLP-Power BI DLP	Low

Alert: DLP-Power BI DLP

Alert ID
ea771ab7-5b89-060c-2e00-08dd9975fd84

Alert status
Active

Alert severity
Low

Time detected
May 22, 2025 5:03 PM

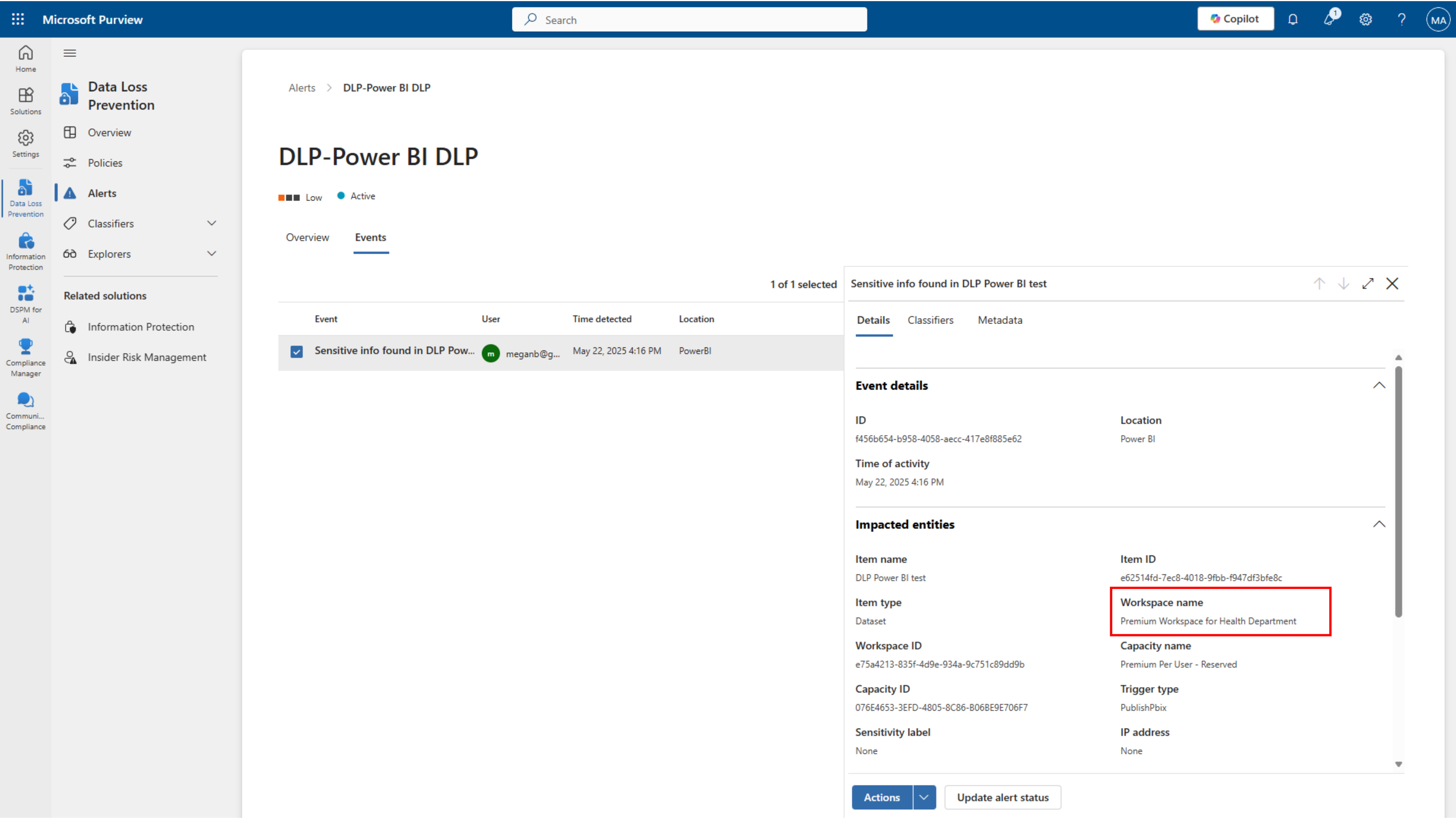
Number of events
1

DLP policy matched
DLP policy for Power BI

Locations
Power BI

Users who performed the event
M Megan Bowen
meganb@gov900497.onmicrosoft.com

Assigned to
No one is assigned



DLP-Power BI DLP

Low · Active

1 of 1 selected

	Event	User	Time detected	Location
☑	Sensitive info found in DLP Pow...	m meganb@g...	May 22, 2025 4:16 PM	PowerBI

Sensitive info found in DLP Power BI test

Event details

ID
f456b654-b958-4058-aecc-417e8f885e62

Location
Power BI

Time of activity
May 22, 2025 4:16 PM

Impacted entities

Item name
DLP Power BI test

Item ID
e62514fd-7ec8-4018-9fbb-f947df3bfe8c

Item type
Dataset

Workspace name
Premium Workspace for Health Department

Workspace ID
e75a4213-835f-4d9e-934a-9c751c89dd9b

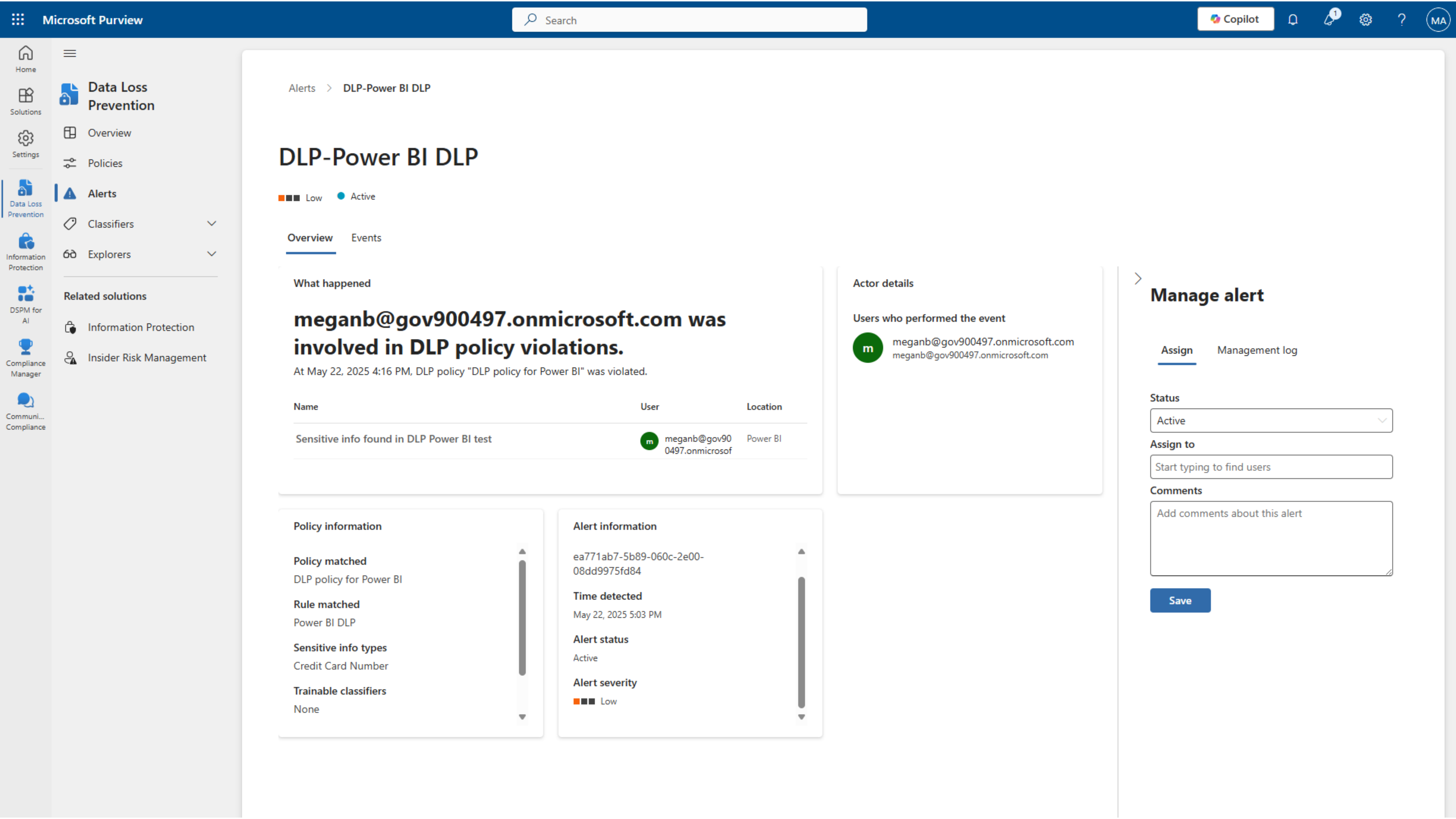
Capacity name
Premium Per User - Reserved

Capacity ID
076E4653-3EFD-4805-8C86-B06BE9E706F7

Trigger type
PublishPbix

Sensitivity label
None

IP address
None



DLP-Power BI DLP

■■■ Low ● Active

Overview Events

What happened

meganb@gov900497.onmicrosoft.com was involved in DLP policy violations.

At May 22, 2025 4:16 PM, DLP policy "DLP policy for Power BI" was violated.

Name	User	Location
Sensitive info found in DLP Power BI test	m meganb@gov900497.onmicrosof	Power BI

Actor details

Users who performed the event

m meganb@gov900497.onmicrosoft.com
meganb@gov900497.onmicrosoft.com

Policy information

Policy matched
DLP policy for Power BI

Rule matched
Power BI DLP

Sensitive info types
Credit Card Number

Trainable classifiers
None

Alert information

ea771ab7-5b89-060c-2e00-08dd9975fd84

Time detected
May 22, 2025 5:03 PM

Alert status
Active

Alert severity
■■■ Low

Manage alert

Assign Management log

Status
Active

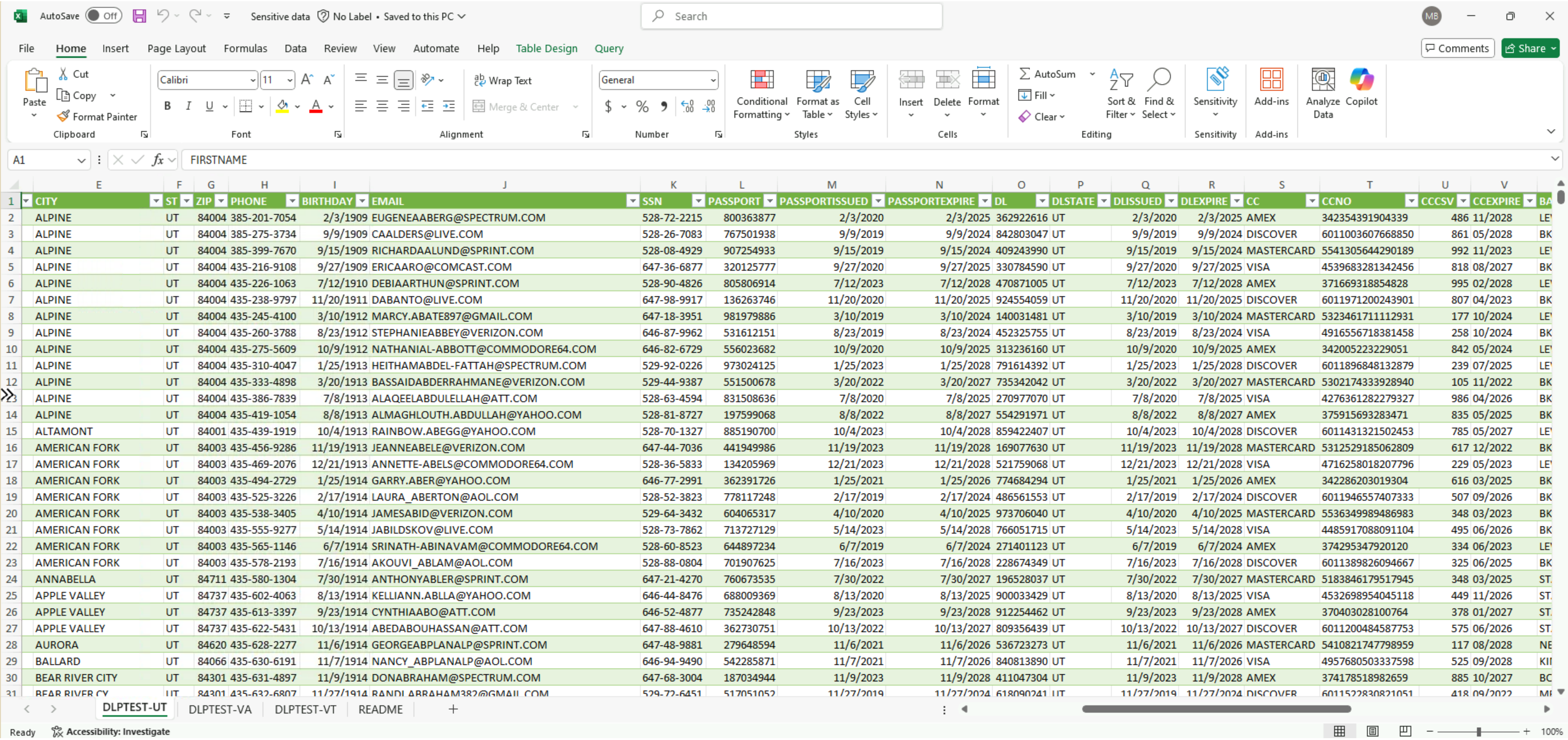
Assign to
Start typing to find users

Comments
Add comments about this alert

Save

DLP –
End User Experience

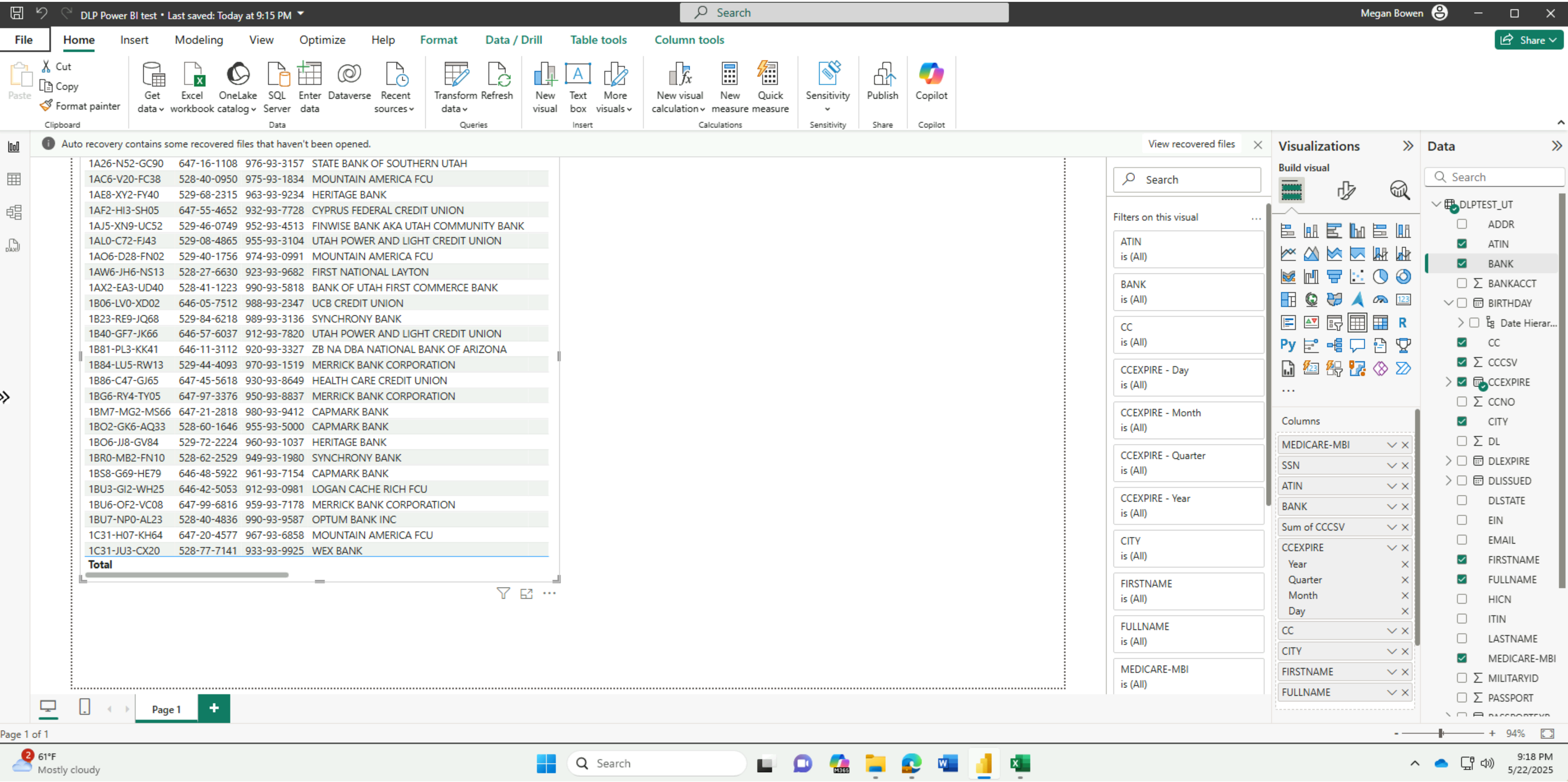
Excel data that contains sensitive info



A1 FIRSTNAME

	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
1	CITY	ST	ZIP	PHONE	BIRTHDAY	EMAIL	SSN	PASSPORT	PASSPORTISSUED	PASSPORTEXPIRE	DL	DLSTATE	DLISSUED	DLEXPIRE	CC	CCNO	CCCSV	CCEXPIRE	BA
2	ALPINE	UT	84004	385-201-7054	2/3/1909	EUGENEAABERG@SPECTRUM.COM	528-72-2215	800363877	2/3/2020	2/3/2025	362922616	UT	2/3/2020	2/3/2025	AMEX	342354391904339	486	11/2028	LE
3	ALPINE	UT	84004	385-275-3734	9/9/1909	CAALDERS@LIVE.COM	528-26-7083	767501938	9/9/2019	9/9/2024	842803047	UT	9/9/2019	9/9/2024	DISCOVER	6011003607668850	861	05/2028	BK
4	ALPINE	UT	84004	385-399-7670	9/15/1909	RICHARDAALUND@SPRINT.COM	528-08-4929	907254933	9/15/2019	9/15/2024	409243990	UT	9/15/2019	9/15/2024	MASTERCARD	5541305644290189	992	11/2023	LE
5	ALPINE	UT	84004	435-216-9108	9/27/1909	ERICAARO@COMCAST.COM	647-36-6877	320125777	9/27/2020	9/27/2025	330784590	UT	9/27/2020	9/27/2025	VISA	4539683281342456	818	08/2027	BK
6	ALPINE	UT	84004	435-226-1063	7/12/1910	DEBIAARTHUN@SPRINT.COM	528-90-4826	805806914	7/12/2023	7/12/2028	470871005	UT	7/12/2023	7/12/2028	AMEX	371669318854828	995	02/2028	LE
7	ALPINE	UT	84004	435-238-9797	11/20/1911	DABANTO@LIVE.COM	647-98-9917	136263746	11/20/2020	11/20/2025	924554059	UT	11/20/2020	11/20/2025	DISCOVER	6011971200243901	807	04/2023	BK
8	ALPINE	UT	84004	435-245-4100	3/10/1912	MARCY.ABATE897@GMAIL.COM	647-18-3951	981979886	3/10/2019	3/10/2024	140031481	UT	3/10/2019	3/10/2024	MASTERCARD	5323461711112931	177	10/2024	LE
9	ALPINE	UT	84004	435-260-3788	8/23/1912	STEPHANIEABBEY@VERIZON.COM	646-87-9962	531612151	8/23/2019	8/23/2024	452325755	UT	8/23/2019	8/23/2024	VISA	4916556718381458	258	10/2024	BK
10	ALPINE	UT	84004	435-275-5609	10/9/1912	NATHANIAL-ABBOTT@COMMODORE64.COM	646-82-6729	556023682	10/9/2020	10/9/2025	313236160	UT	10/9/2020	10/9/2025	AMEX	342005223229051	842	05/2024	LE
11	ALPINE	UT	84004	435-310-4047	1/25/1913	HEITHAMABDEL-FATTAH@SPECTRUM.COM	529-92-0226	973024125	1/25/2023	1/25/2028	791614392	UT	1/25/2023	1/25/2028	DISCOVER	6011896848132879	239	07/2025	LE
12	ALPINE	UT	84004	435-333-4898	3/20/1913	BASSAIDABDERRAHMANE@VERIZON.COM	529-44-9387	551500678	3/20/2022	3/20/2027	735342042	UT	3/20/2022	3/20/2027	MASTERCARD	5302174333928940	105	11/2022	BK
13	ALPINE	UT	84004	435-386-7839	7/8/1913	ALAQEELABDULELLAH@ATT.COM	528-63-4594	831508636	7/8/2020	7/8/2025	270977070	UT	7/8/2020	7/8/2025	VISA	4276361282279327	986	04/2026	BK
14	ALPINE	UT	84004	435-419-1054	8/8/1913	ALMAGHLOUTH.ABDULLAH@YAHOO.COM	528-81-8727	197599068	8/8/2022	8/8/2027	554291971	UT	8/8/2022	8/8/2027	AMEX	375915693283471	835	05/2025	BK
15	ALTAMONT	UT	84001	435-439-1919	10/4/1913	RAINBOW.ABEGG@YAHOO.COM	528-70-1327	885190700	10/4/2023	10/4/2028	859422407	UT	10/4/2023	10/4/2028	DISCOVER	6011431321502453	785	05/2027	LE
16	AMERICAN FORK	UT	84003	435-456-9286	11/19/1913	JEANNEABELE@VERIZON.COM	647-44-7036	441949986	11/19/2023	11/19/2028	169077630	UT	11/19/2023	11/19/2028	MASTERCARD	5312529185062809	617	12/2022	BK
17	AMERICAN FORK	UT	84003	435-469-2076	12/21/1913	ANNETTE-ABELS@COMMODORE64.COM	528-36-5833	134205969	12/21/2023	12/21/2028	521759068	UT	12/21/2023	12/21/2028	VISA	4716258018207796	229	05/2023	LE
18	AMERICAN FORK	UT	84003	435-494-2729	1/25/1914	GARRY.ABER@YAHOO.COM	646-77-2991	362391726	1/25/2021	1/25/2026	774684294	UT	1/25/2021	1/25/2026	AMEX	342286203019304	616	03/2025	BK
19	AMERICAN FORK	UT	84003	435-525-3226	2/17/1914	LAURA_ABERTON@AOL.COM	528-52-3823	778117248	2/17/2019	2/17/2024	486561553	UT	2/17/2019	2/17/2024	DISCOVER	6011946557407333	507	09/2026	BK
20	AMERICAN FORK	UT	84003	435-538-3405	4/10/1914	JAMESABID@VERIZON.COM	529-64-3432	604065317	4/10/2020	4/10/2025	973706040	UT	4/10/2020	4/10/2025	MASTERCARD	5536349989486983	348	03/2023	BK
21	AMERICAN FORK	UT	84003	435-555-9277	5/14/1914	JABILDSKOV@LIVE.COM	528-73-7862	713727129	5/14/2023	5/14/2028	766051715	UT	5/14/2023	5/14/2028	VISA	4485917088091104	495	06/2026	BK
22	AMERICAN FORK	UT	84003	435-565-1146	6/7/1914	SRINATH-ABINAVAM@COMMODORE64.COM	528-60-8523	644897234	6/7/2019	6/7/2024	271401123	UT	6/7/2019	6/7/2024	AMEX	374295347920120	334	06/2023	LE
23	AMERICAN FORK	UT	84003	435-578-2193	7/16/1914	AKOUVI_ABLAM@AOL.COM	528-88-0804	701907625	7/16/2023	7/16/2028	228674349	UT	7/16/2023	7/16/2028	DISCOVER	6011389826094667	325	06/2025	BK
24	ANNABELLA	UT	84711	435-580-1304	7/30/1914	ANTHONYABLER@SPRINT.COM	647-21-4270	760673535	7/30/2022	7/30/2027	196528037	UT	7/30/2022	7/30/2027	MASTERCARD	5183846179517945	348	03/2025	ST.
25	APPLE VALLEY	UT	84737	435-602-4063	8/13/1914	KELLIANN.ABLLA@YAHOO.COM	646-44-8476	688009369	8/13/2020	8/13/2025	900033429	UT	8/13/2020	8/13/2025	VISA	4532698954045118	449	11/2026	ST.
26	APPLE VALLEY	UT	84737	435-613-3397	9/23/1914	CYNTHIAABO@ATT.COM	646-52-4877	735242848	9/23/2023	9/23/2028	912254462	UT	9/23/2023	9/23/2028	AMEX	370403028100764	378	01/2027	ST.
27	APPLE VALLEY	UT	84737	435-622-5431	10/13/1914	ABEDABOUHASSAN@ATT.COM	647-88-4610	362730751	10/13/2022	10/13/2027	809356439	UT	10/13/2022	10/13/2027	DISCOVER	6011200484587753	575	06/2026	ST.
28	AURORA	UT	84620	435-628-2277	11/6/1914	GEORGEABPLANALP@SPRINT.COM	647-48-9881	279648594	11/6/2021	11/6/2026	536723273	UT	11/6/2021	11/6/2026	MASTERCARD	5410821747798959	117	08/2028	NE
29	BALLARD	UT	84066	435-630-6191	11/7/1914	NANCY_ABPLANALP@AOL.COM	646-94-9490	542285871	11/7/2021	11/7/2026	840813890	UT	11/7/2021	11/7/2026	VISA	4957680503337598	525	09/2028	KI
30	BEAR RIVER CITY	UT	84301	435-631-4897	11/9/1914	DONABRAHAM@SPECTRUM.COM	647-68-3004	187034944	11/9/2023	11/9/2028	411047304	UT	11/9/2023	11/9/2028	AMEX	374178518982659	885	10/2027	BC
31	BEAR RIVER CY	UT	84301	435-632-6807	11/27/1914	RANDI.ABRAHAM382@GMAIL.COM	529-72-6451	517051052	11/27/2019	11/27/2024	618090241	UT	11/27/2019	11/27/2024	DISCOVER	6011522830821051	418	09/2022	MI

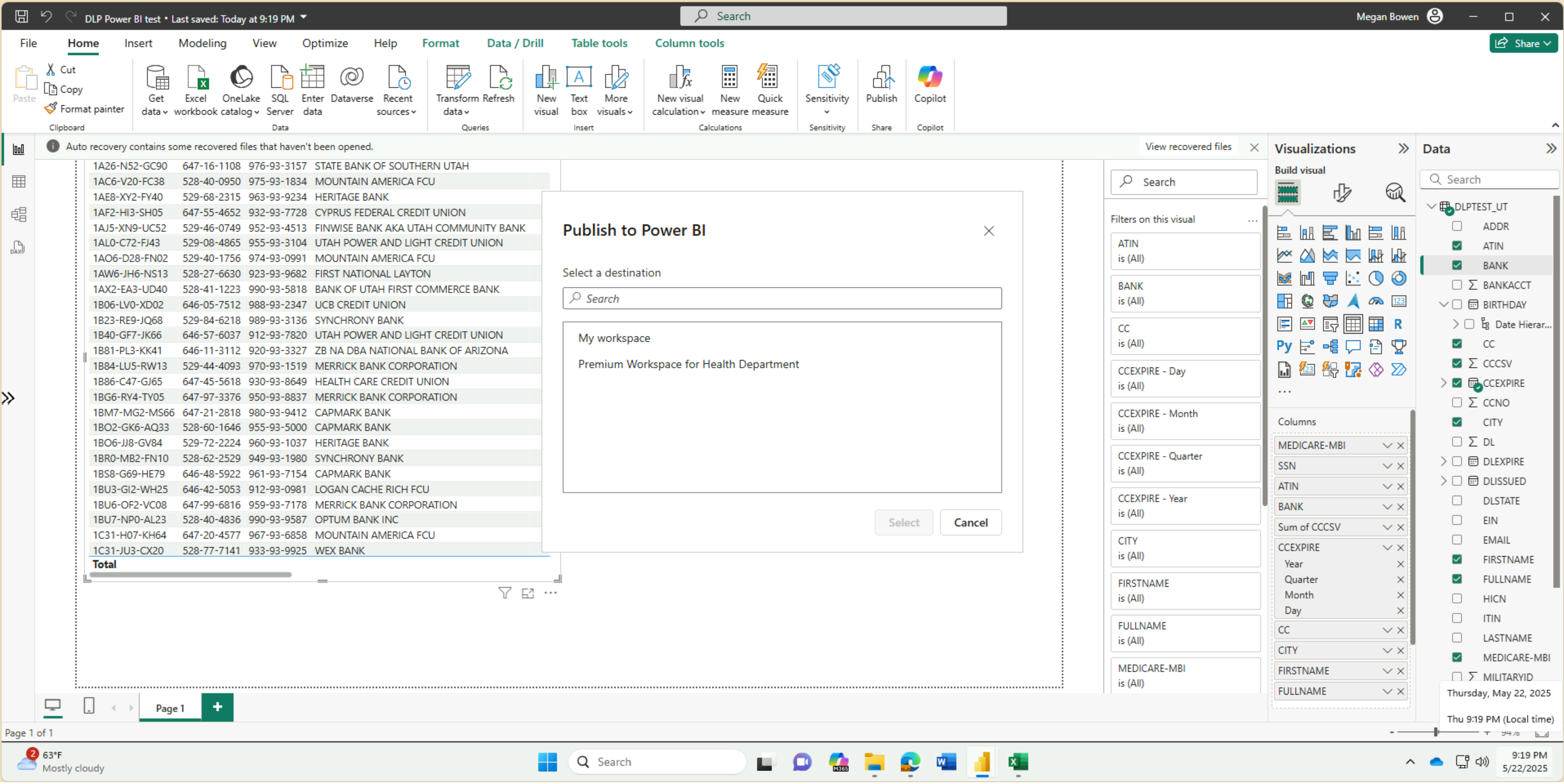
Power BI report created from the sensitive data source



Auto recovery contains some recovered files that haven't been opened.

1A26-N52-GC90	647-16-1108	976-93-3157	STATE BANK OF SOUTHERN UTAH
1AC6-V20-FC38	528-40-0950	975-93-1834	MOUNTAIN AMERICA FCU
1AE8-XY2-FY40	529-68-2315	963-93-9234	HERITAGE BANK
1AF2-HI3-SH05	647-55-4652	932-93-7728	CYPRUS FEDERAL CREDIT UNION
1AJ5-XN9-UC52	529-46-0749	952-93-4513	FINWISE BANK AKA UTAH COMMUNITY BANK
1AL0-C72-FJ43	529-08-4865	955-93-3104	UTAH POWER AND LIGHT CREDIT UNION
1AO6-D28-FN02	529-40-1756	974-93-0991	MOUNTAIN AMERICA FCU
1AW6-JH6-NS13	528-27-6630	923-93-9682	FIRST NATIONAL LAYTON
1AX2-EA3-UD40	528-41-1223	990-93-5818	BANK OF UTAH FIRST COMMERCE BANK
1B06-LV0-XD02	646-05-7512	988-93-2347	UCB CREDIT UNION
1B23-RE9-JQ68	529-84-6218	989-93-3136	SYNCHRONY BANK
1B40-GF7-JK66	646-57-6037	912-93-7820	UTAH POWER AND LIGHT CREDIT UNION
1B81-PL3-KK41	646-11-3112	920-93-3327	ZB NA DBA NATIONAL BANK OF ARIZONA
1B84-LU5-RW13	529-44-4093	970-93-1519	MERRICK BANK CORPORATION
1B86-C47-GJ65	647-45-5618	930-93-8649	HEALTH CARE CREDIT UNION
1BG6-RY4-TY05	647-97-3376	950-93-8837	MERRICK BANK CORPORATION
1BM7-MG2-MS66	647-21-2818	980-93-9412	CAPMARK BANK
1BO2-GK6-AQ33	528-60-1646	955-93-5000	CAPMARK BANK
1BO6-JJ8-GV84	529-72-2224	960-93-1037	HERITAGE BANK
1BR0-MB2-FN10	528-62-2529	949-93-1980	SYNCHRONY BANK
1BS8-G69-HE79	646-48-5922	961-93-7154	CAPMARK BANK
1BU3-GI2-WH25	646-42-5053	912-93-0981	LOGAN CACHE RICH FCU
1BU6-OF2-VC08	647-99-6816	959-93-7178	MERRICK BANK CORPORATION
1BU7-NP0-AL23	528-40-4836	990-93-9587	OPTUM BANK INC
1C31-H07-KH64	647-20-4577	967-93-6858	MOUNTAIN AMERICA FCU
1C31-JU3-CX20	528-77-7141	933-93-9925	WEX BANK
Total			

Power BI report published to Workspace



Auto recovery contains some recovered files that haven't been opened.

1A26-N52-GC90	647-16-1108	976-93-3157	STATE BANK OF SOUTHERN UTAH
1AC6-V20-FC38	528-40-0950	975-93-1834	MOUNTAIN AMERICA FCU
1AE8-XY2-FY40	529-68-2315	963-93-9234	HERITAGE BANK
1AF2-HI3-SH05	647-55-4652	932-93-7728	CYPRUS FEDERAL CREDIT UNION
1AJ5-XN9-UC52	529-46-0749	952-93-4513	FINWISE BANK AKA UTAH COMMUNITY BANK
1AL0-C72-FJ43	529-08-4865	955-93-3104	UTAH POWER AND LIGHT CREDIT UNION
1AO6-D28-FN02	529-40-1756	974-93-0991	MOUNTAIN AMERICA FCU
1AW6-JH6-NS13	528-27-6630	923-93-9682	FIRST NATIONAL LAYTON
1AX2-EA3-UD40	528-41-1223	990-93-5818	BANK OF UTAH FIRST COMMERCE BANK
1B06-LV0-XD02	646-05-7512	988-93-2347	UCB CREDIT UNION
1B23-RE9-JQ68	529-84-6218	989-93-3136	SYNCHRONY BANK
1B40-GF7-JK66	646-57-6037	912-93-7820	UTAH POWER AND LIGHT CREDIT UNION
1B81-PL3-KK41	646-11-3112	920-93-3327	ZB NA DBA NATIONAL BANK OF ARIZONA
1B84-LU5-RW13	529-44-4093	970-93-1519	MERRICK BANK CORPORATION
1B86-C47-GJ65	647-45-5618	930-93-8649	HEALTH CARE CREDIT UNION
1BG6-RY4-TY05	647-97-3376	950-93-8837	MERRICK BANK CORPORATION
1BM7-MG2-MS66	647-21-2818	980-93-9412	CAPMARK BANK
1BO2-GK6-AQ33	528-60-1646	955-93-5000	CAPMARK BANK
1BO6-JJ8-GV84	529-72-2224	960-93-1037	HERITAGE BANK
1BR0-MB2-FN10	528-62-2529	949-93-1980	SYNCHRONY BANK
1BS8-G69-HE79	646-48-5922	961-93-7154	CAPMARK BANK
1BU3-GI2-WH25	646-42-5053	912-93-0981	LOGAN CACHE RICH FCU
1BU6-OF2-VC08	647-99-6816	959-93-7178	MERRICK BANK CORPORATION
1BU7-NP0-AL23	528-40-4836	990-93-9587	OPTUM BANK INC
1C31-H07-KH64	647-20-4577	967-93-6858	MOUNTAIN AMERICA FCU
1C31-JU3-CX20	528-77-7141	933-93-9925	WEX BANK
Total			

Publish to Power BI

Select a destination

Search

My workspace

Premium Workspace for Health Department

Select | Cancel

Filters on this visual:

- ATIN is (All)
- BANK is (All)
- CC is (All)
- CCEXPIRE - Day is (All)
- CCEXPIRE - Month is (All)
- CCEXPIRE - Quarter is (All)
- CCEXPIRE - Year is (All)
- CITY is (All)
- FIRSTNAME is (All)
- FULLNAME is (All)
- MEDICARE-MBI is (All)

Columns:

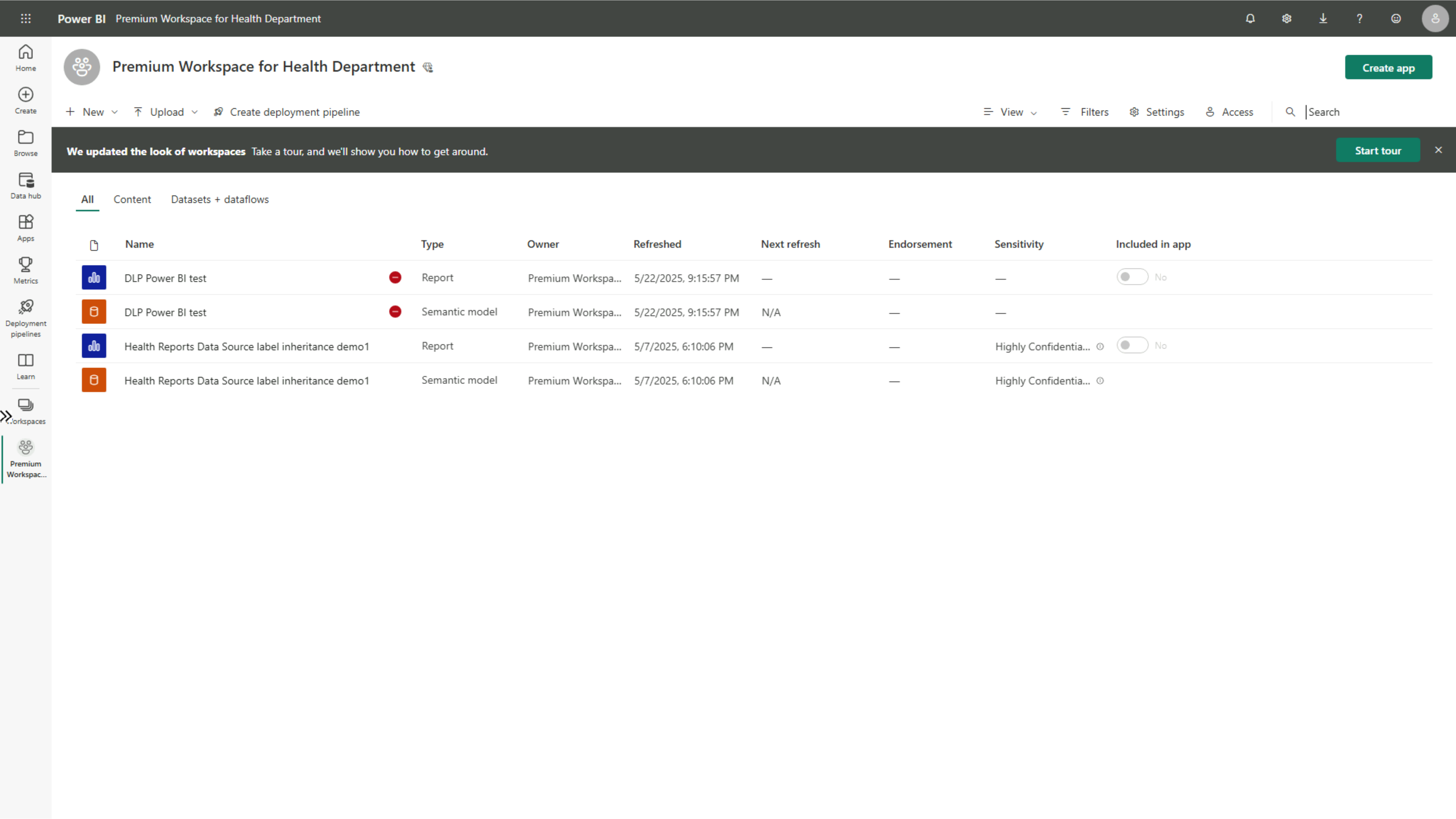
- MEDICARE-MBI
- SSN
- ATIN
- BANK
- Sum of CCCSV
- CCEXPIRE
  - Year
  - Quarter
  - Month
  - Day
- CC
- CITY
- FIRSTNAME
- FULLNAME

Data:

- DLPTEST_UT
  - ☐ ADDR
  - ☑ ATIN
  - ☑ BANK
  - ☐ Σ BANKACCT
  - ☐ BIRTHDAY
    - ☐ Date Hierar...
  - ☑ CC
  - ☑ Σ CCCSV
  - ☑ CCEXPIRE
  - ☐ Σ CCNO
  - ☑ CITY
  - ☐ Σ DL
  - ☐ DLEXPIRE
  - ☐ DLISSUED
  - ☐ DLSTATE
  - ☐ EIN
  - ☐ EMAIL
  - ☑ FIRSTNAME
  - ☑ FULLNAME
  - ☐ HICN
  - ☐ ITIN
  - ☐ LASTNAME
  - ☑ MEDICARE-MBI
  - ☐ Σ MILITARYID

Thursday, May 22, 2025

Thu 9:19 PM (Local time)

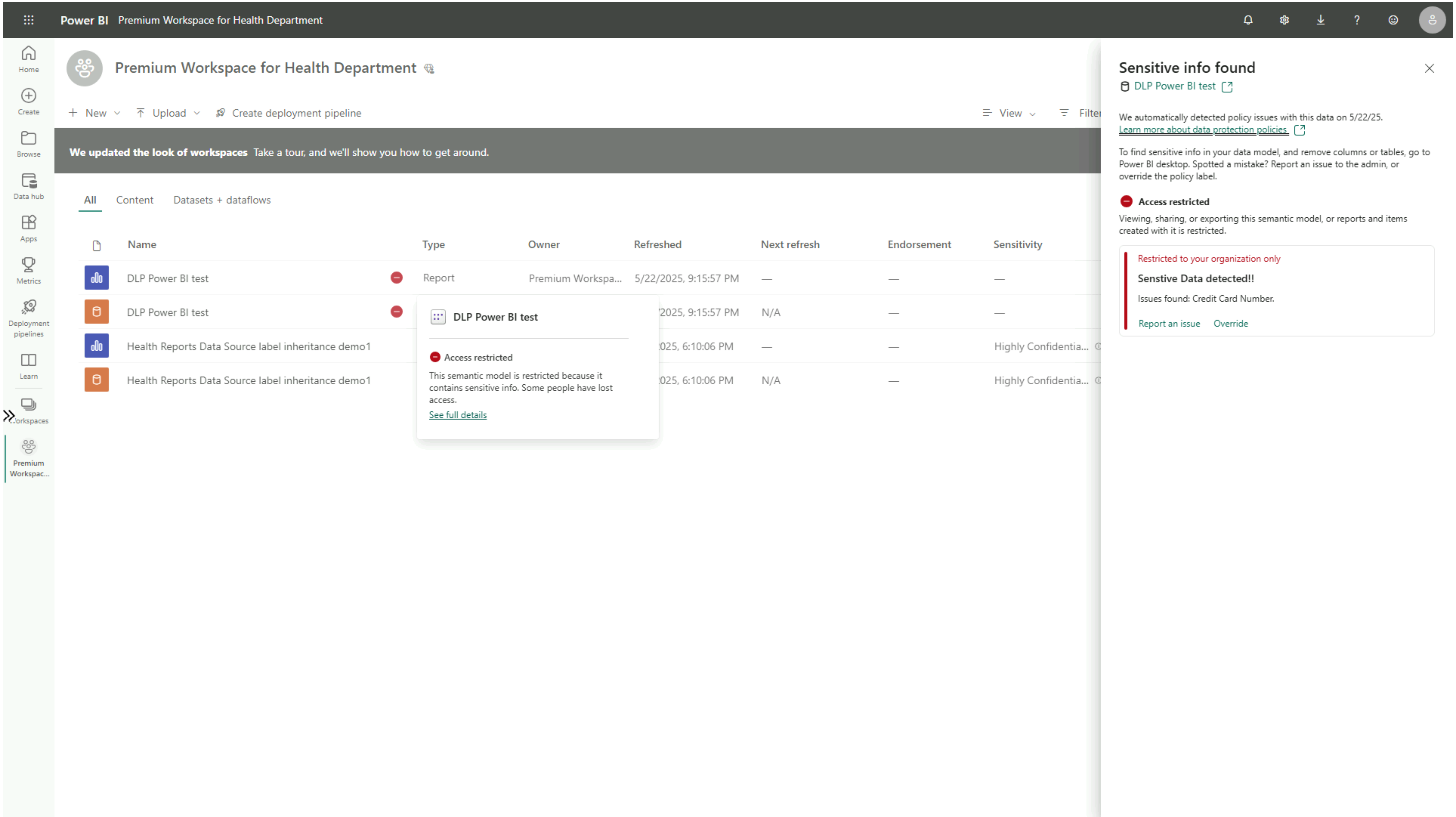


Premium Workspace for Health Department

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	Included in app
DLP Power BI test	⛔	Report	Premium Workspa...	5/22/2025, 9:15:57 PM	—	—	—	No
DLP Power BI test	⛔	Semantic model	Premium Workspa...	5/22/2025, 9:15:57 PM	N/A	—	—	
Health Reports Data Source label inheritance demo1		Report	Premium Workspa...	5/7/2025, 6:10:06 PM	—	—	Highly Confidentia...	No
Health Reports Data Source label inheritance demo1		Semantic model	Premium Workspa...	5/7/2025, 6:10:06 PM	N/A	—	Highly Confidentia...	

Power BI data set inside the workspace



Premium Workspace for Health Department

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
DLP Power BI test	Report	Premium Workspa...	5/22/2025, 9:15:57 PM	—	—	—
DLP Power BI test			/2025, 9:15:57 PM	N/A	—	—
Health Reports Data Source label inheritance demo1			025, 6:10:06 PM	—	—	Highly Confidentia...
Health Reports Data Source label inheritance demo1			025, 6:10:06 PM	N/A	—	Highly Confidentia...

DLP Power BI test

Access restricted

This semantic model is restricted because it contains sensitive info. Some people have lost access.

See full details

Sensitive info found

DLP Power BI test

We automatically detected policy issues with this data on 5/22/25.
Learn more about data protection policies

To find sensitive info in your data model, and remove columns or tables, go to Power BI desktop. Spotted a mistake? Report an issue to the admin, or override the policy label.

Access restricted

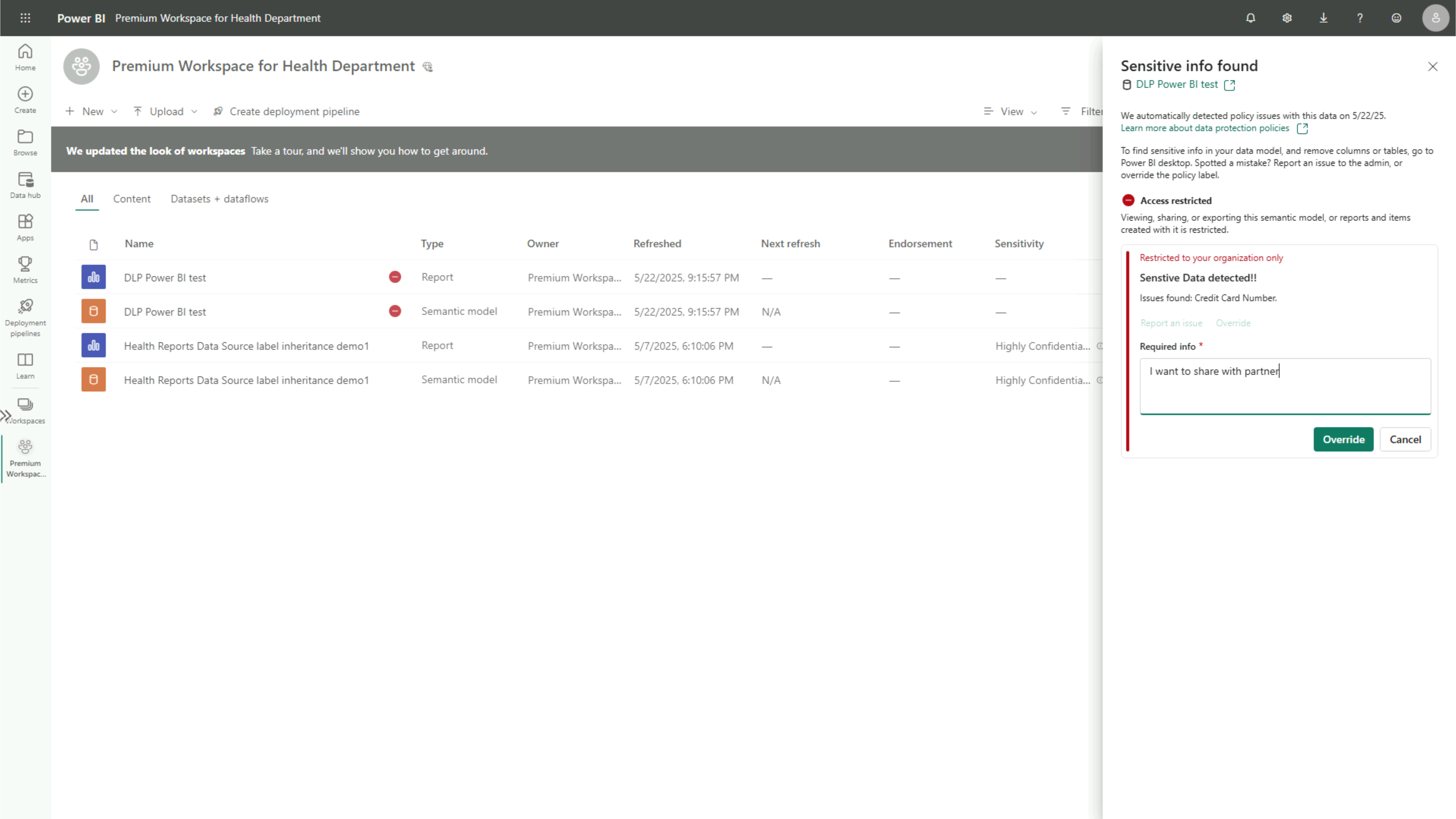
Viewing, sharing, or exporting this semantic model, or reports and items created with it is restricted.

Restricted to your organization only

Senstive Data detected!!

Issues found: Credit Card Number.

Report an issue   Override



Premium Workspace for Health Department

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
DLP Power BI test	⛔	Report	Premium Workspa...	5/22/2025, 9:15:57 PM	—	—	—
DLP Power BI test	⛔	Semantic model	Premium Workspa...	5/22/2025, 9:15:57 PM	N/A	—	—
Health Reports Data Source label inheritance demo1		Report	Premium Workspa...	5/7/2025, 6:10:06 PM	—	—	Highly Confidentia...
Health Reports Data Source label inheritance demo1		Semantic model	Premium Workspa...	5/7/2025, 6:10:06 PM	N/A	—	Highly Confidentia...

Sensitive info found

DLP Power BI test

We automatically detected policy issues with this data on 5/22/25.
Learn more about data protection policies

To find sensitive info in your data model, and remove columns or tables, go to Power BI desktop. Spotted a mistake? Report an issue to the admin, or override the policy label.

⛔ **Access restricted**

Viewing, sharing, or exporting this semantic model, or reports and items created with it is restricted.

Restricted to your organization only

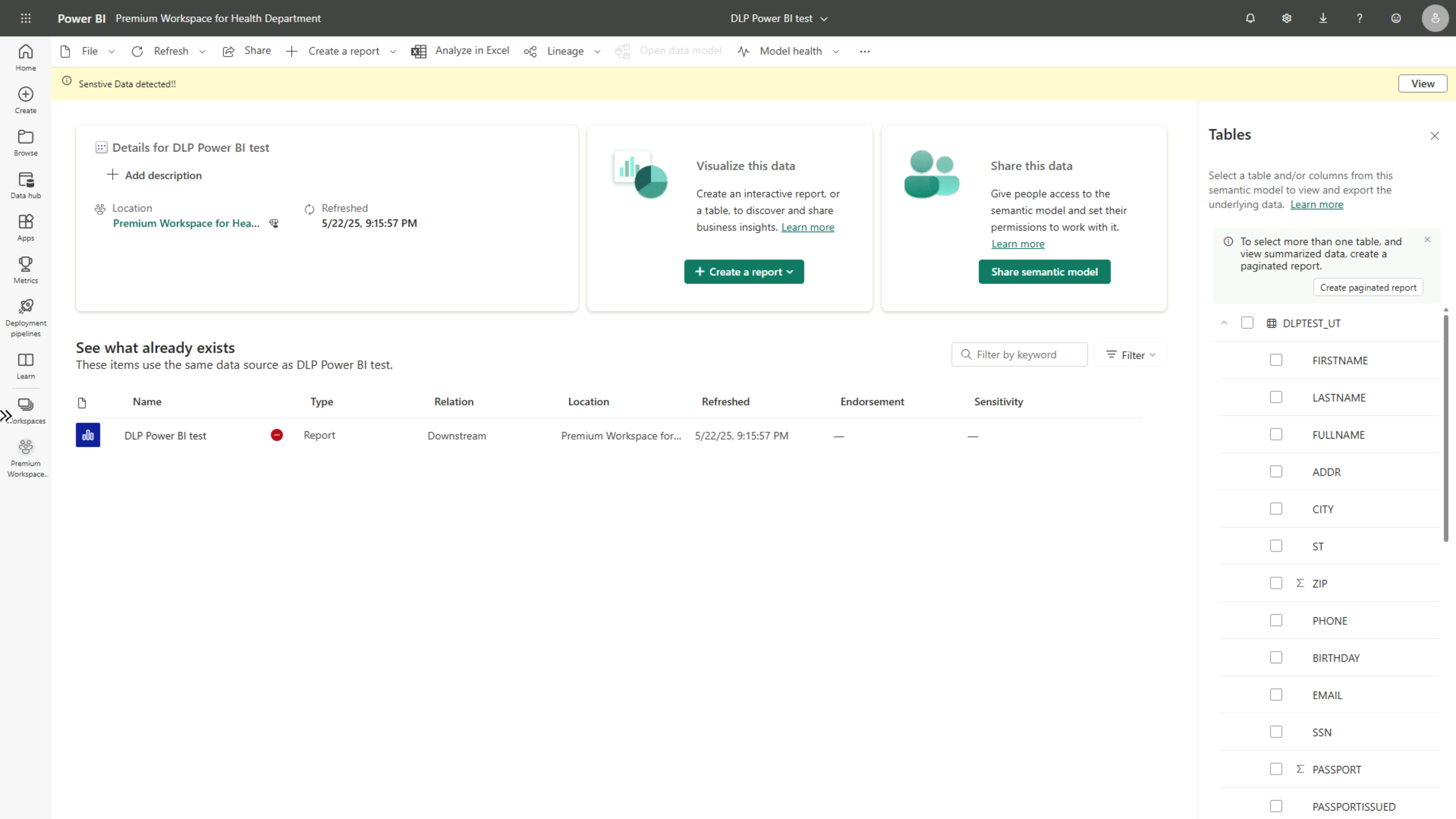
Senstive Data detected!!

Issues found: Credit Card Number.

Report an issue   Override

Required info *

I want to share with partner



Senstive Data detected!!

Details for DLP Power BI test

+ Add description

Location
Premium Workspace for Hea...

Refreshed
5/22/25, 9:15:57 PM

Visualize this data

Create an interactive report, or a table, to discover and share business insights. Learn more

+ Create a report

Share this data

Give people access to the semantic model and set their permissions to work with it. Learn more

Share semantic model

See what already exists

These items use the same data source as DLP Power BI test.

Filter by keyword

Filter

Name	Type	Relation	Location	Refreshed	Endorsement	Sensitivity
DLP Power BI test	Report	Downstream	Premium Workspace for...	5/22/25, 9:15:57 PM	—	—

Tables

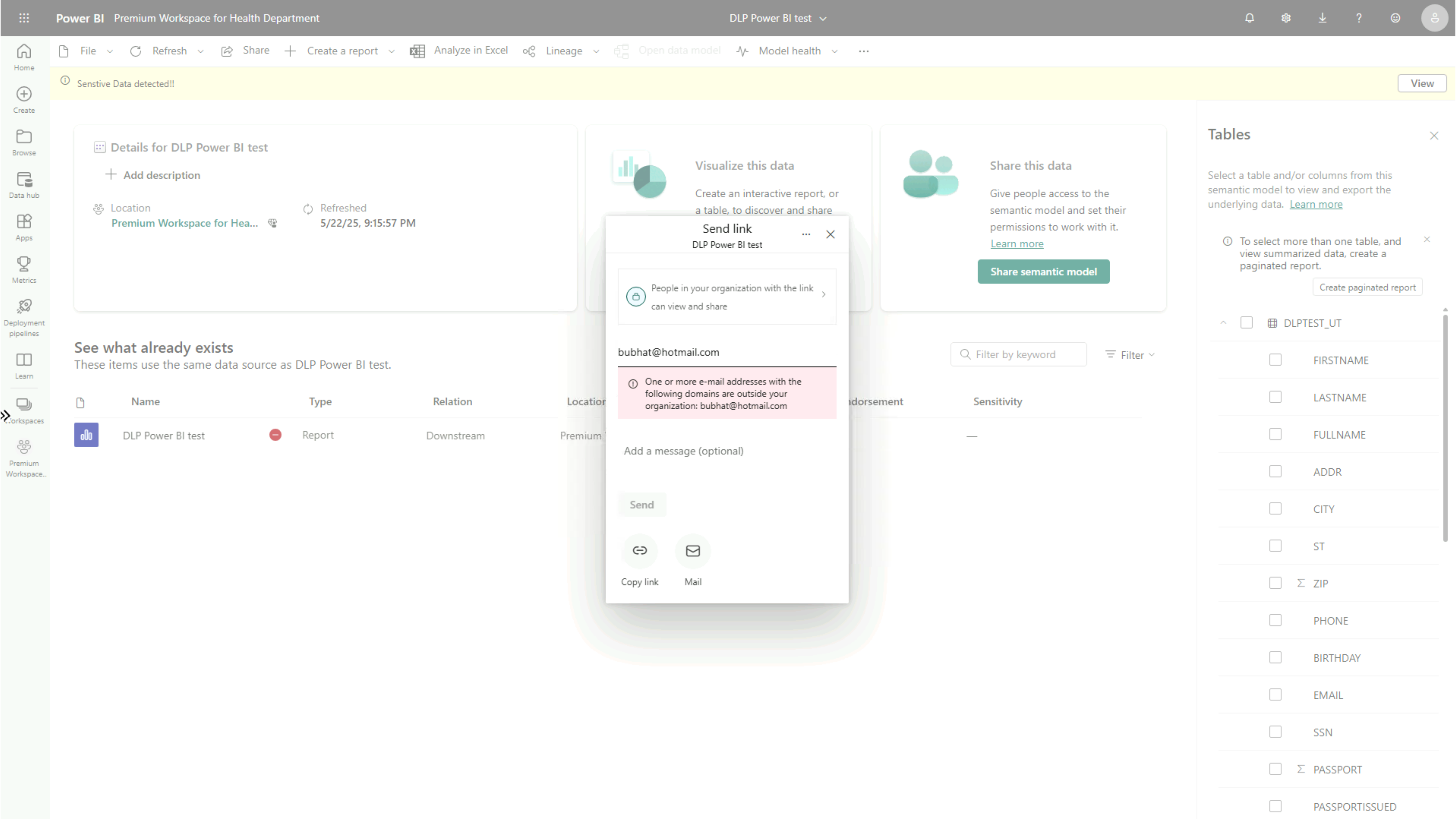
Select a table and/or columns from this semantic model to view and export the underlying data. Learn more

To select more than one table, and view summarized data, create a paginated report.

Create paginated report

□ DLPTEST_UT

- □ FIRSTNAME
- □ LASTNAME
- □ FULLNAME
- □ ADDR
- □ CITY
- □ ST
- □ Σ ZIP
- □ PHONE
- □ BIRTHDAY
- □ EMAIL
- □ SSN
- □ Σ PASSPORT
- □ PASSPORTISSUED



Senstive Data detected!!

Details for DLP Power BI test

Location: Premium Workspace for Hea...

Refreshed: 5/22/25, 9:15:57 PM

Create an interactive report, or a table, to discover and share

Give people access to the semantic model and set their permissions to work with it. Learn more

See what already exists

These items use the same data source as DLP Power BI test.

Name	Type	Relation	Locatior	ndorsement	Sensitivity
DLP Power BI test	Report	Downstream	Premium		—

Send link

DLP Power BI test

People in your organization with the link can view and share

bubhat@hotmail.com

One or more e-mail addresses with the following domains are outside your organization: bubhat@hotmail.com

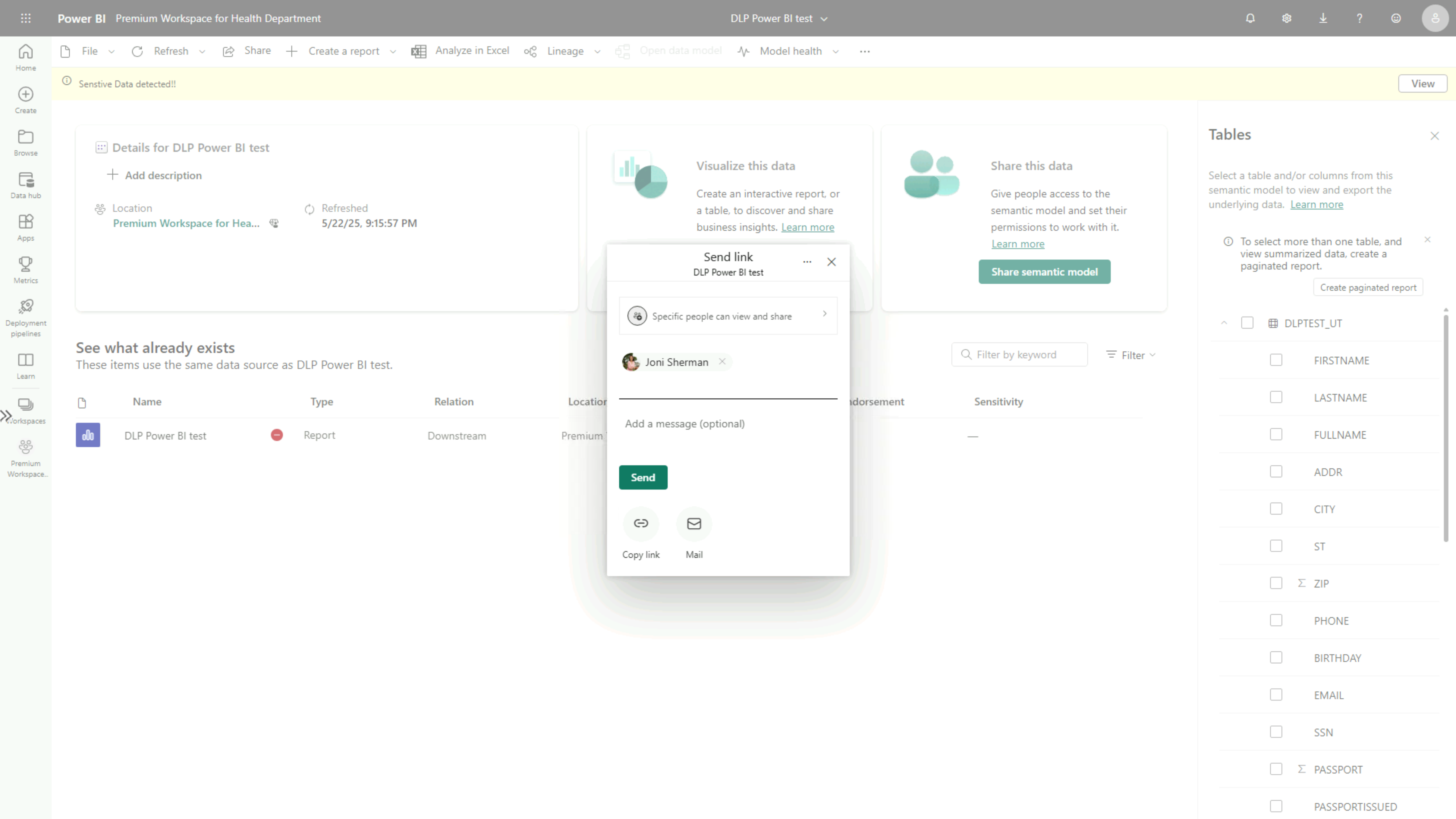
Add a message (optional)

Tables

Select a table and/or columns from this semantic model to view and export the underlying data. Learn more

To select more than one table, and view summarized data, create a paginated report.

- □ DLPTEST_UT
  - □ FIRSTNAME
  - □ LASTNAME
  - □ FULLNAME
  - □ ADDR
  - □ CITY
  - □ ST
  - □ Σ ZIP
  - □ PHONE
  - □ BIRTHDAY
  - □ EMAIL
  - □ SSN
  - □ Σ PASSPORT
  - □ PASSPORTISSUED



Power BI Premium Workspace for Health Department

DLP Power BI test

File · Refresh · Share · Create a report · Analyze in Excel · Lineage · Open data model · Model health · ···

Home · Create · Browse · Data hub · Apps · Metrics · Deployment pipelines · Learn · Workspaces · Premium Workspace...

ⓘ Senstive Data detected!!

View

Details for DLP Power BI test

+ Add description

Location

Premium Workspace for Hea...

Refreshed

5/22/25, 9:15:57 PM

Visualize this data

Create an interactive report, or a table, to discover and share business insights. Learn more

Share this data

Give people access to the semantic model and set their permissions to work with it. Learn more

Share semantic model

See what already exists

These items use the same data source as DLP Power BI test.

Name		Type	Relation	Location	Endorsement	Sensitivity
DLP Power BI test	⛔	Report	Downstream	Premium		—

Filter by keyword · Filter

Send link

DLP Power BI test

Specific people can view and share

Joni Sherman ✕

Add a message (optional)

Send

Copy link · Mail

Tables

Select a table and/or columns from this semantic model to view and export the underlying data. Learn more

ⓘ To select more than one table, and view summarized data, create a paginated report.

Create paginated report

- □ DLPTEST_UT
  - □ FIRSTNAME
  - □ LASTNAME
  - □ FULLNAME
  - □ ADDR
  - □ CITY
  - □ ST
  - □ Σ ZIP
  - □ PHONE
  - □ BIRTHDAY
  - □ EMAIL
  - □ SSN
  - □ Σ PASSPORT
  - □ PASSPORTISSUED

Microsoft Defender for Cloud Apps for Power BI

Using Cloud App Security, it is possible to detect and control risky Power BI sessions in real time, thus reducing the chance of damage that could be caused by content and data being accessed by malicious actors.

Defender for Cloud Apps Policies for Power BI

Monitor, block, or control user sessions in real time.

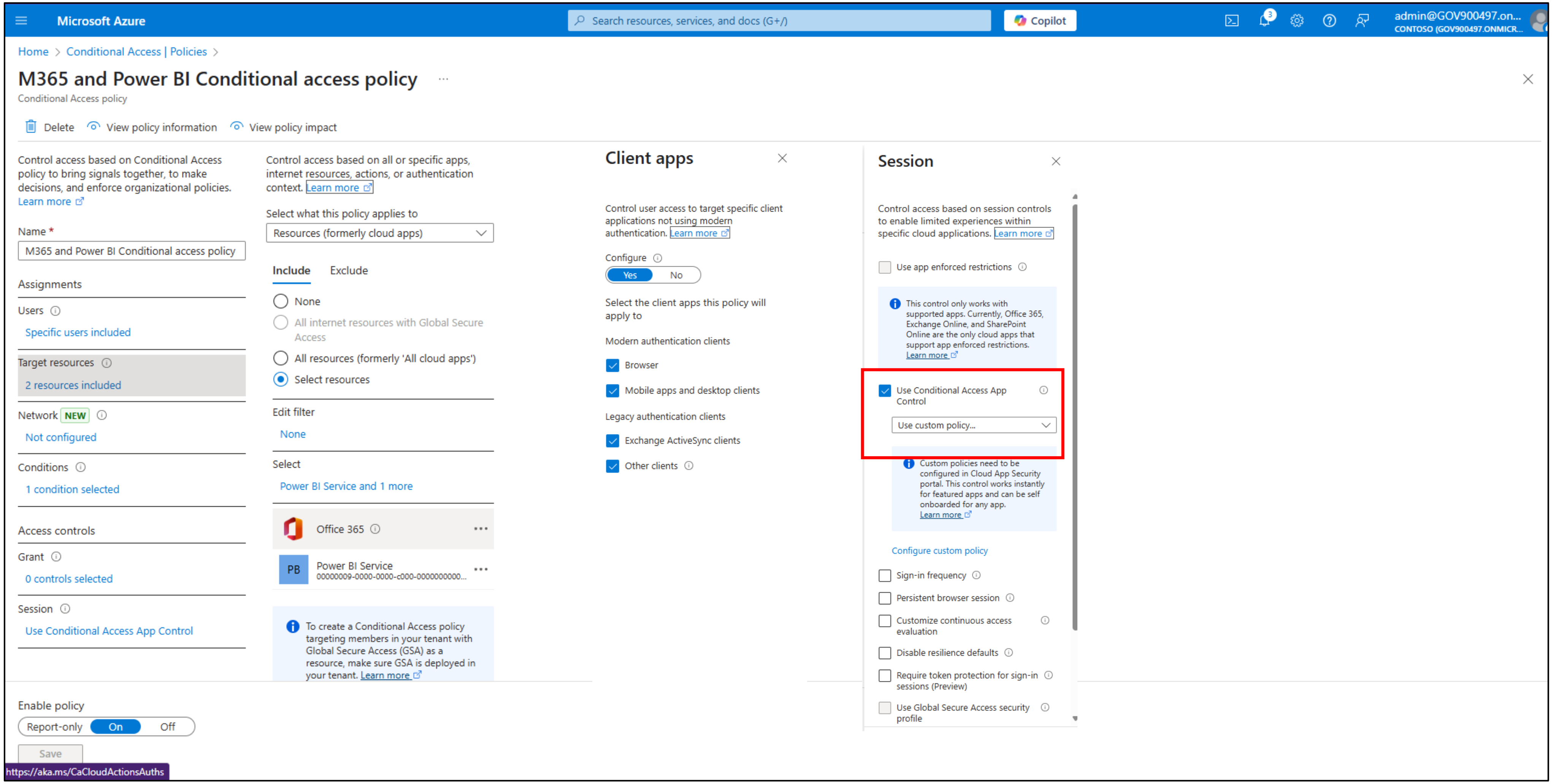
- **Access Policies** - Controls whether a user is allowed to sign in to a cloud application like the Power BI service.

- **Session Policies** - Allows access for the user while monitoring or limiting what actively occurs during their session.

Monitor and act on activities recorded in Power BI activity log (Non-Real time policies)

- **Activity policies** – Take Governance actions based on a single or repeated activity already performed by the user

Create Conditional access policies in Microsoft Entra ID


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
3
admin@GOV900497.on...
CONTOSO (GOV900497.ONMICR...
Home > Conditional Access | Policies >
Delete
View policy information
View policy impact

M365 and Power BI Conditional access policy

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and to enforce organizational policies. Learn more

Name *

M365 and Power BI Conditional access policy

Assignments

Users ⓘ

Specific users included

Target resources ⓘ

2 resources included

Network NEW ⓘ

Not configured

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

Use Conditional Access App Control

Enable policy

Report-only [✓ On] Off

Save

https://aka.ms/CaCloudActionsAuths

Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more

Select what this policy applies to

Resources (formerly cloud apps)

Include Exclude

○ None

○ All internet resources with Global Secure Access

○ All resources (formerly 'All cloud apps')

● Select resources

Edit filter

None

Select

Power BI Service and 1 more

	Office 365 ⓘ	···
PB	Power BI Service 00000009-0000-0000-c000-000000000...	···

ⓘ To create a Conditional Access policy targeting members in your tenant with Global Secure Access (GSA) as a resource, make sure GSA is deployed in your tenant. Learn more

Client apps

Control user access to target specific client applications not using modern authentication. Learn more

Configure ⓘ

[✓ Yes] No

Select the client apps this policy will apply to

Modern authentication clients

☑ Browser

☑ Mobile apps and desktop clients

Legacy authentication clients

☑ Exchange ActiveSync clients

☑ Other clients ⓘ

Session

Control access based on session controls to enable limited experiences within specific cloud applications. Learn more

□ Use app enforced restrictions ⓘ

ⓘ This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Learn more

☑ Use Conditional Access App Control ⓘ

Use custom policy...

ⓘ Custom policies need to be configured in Cloud App Security portal. This control works instantly for featured apps and can be self onboarded for any app. Learn more

Configure custom policy

□ Sign-in frequency ⓘ

□ Persistent browser session ⓘ

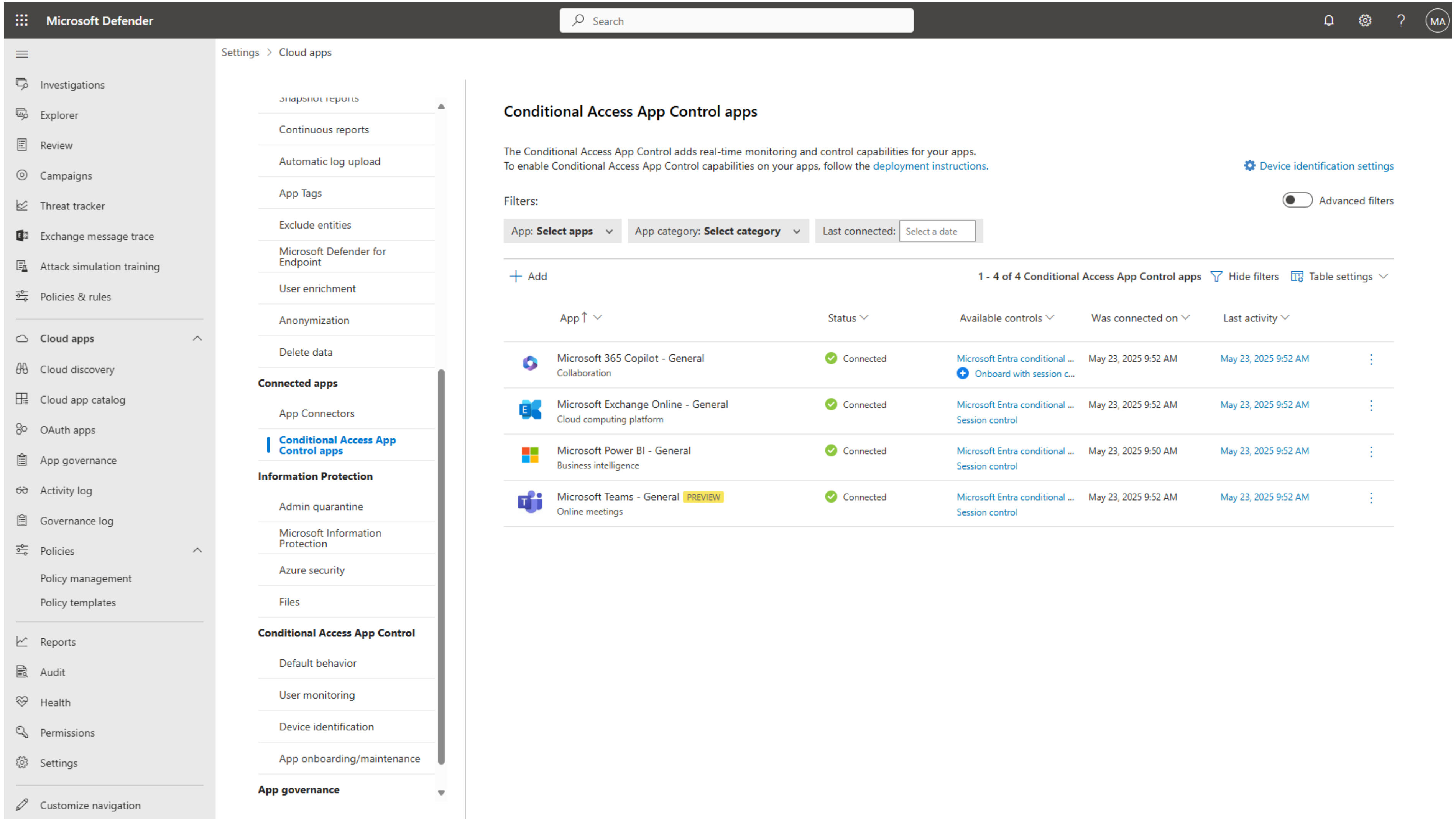
□ Customize continuous access evaluation ⓘ

□ Disable resilience defaults ⓘ

□ Require token protection for sign-in sessions (Preview) ⓘ

□ Use Global Secure Access security profile ⓘ

Defender for Cloud Apps – Conditional Access App control



Conditional Access App Control apps

The Conditional Access App Control adds real-time monitoring and control capabilities for your apps.
To enable Conditional Access App Control capabilities on your apps, follow the deployment instructions.

Device identification settings

Filters:

Advanced filters

App: **Select apps** | App category: **Select category** | Last connected: Select a date

+ Add

1 - 4 of 4 Conditional Access App Control apps Hide filters Table settings

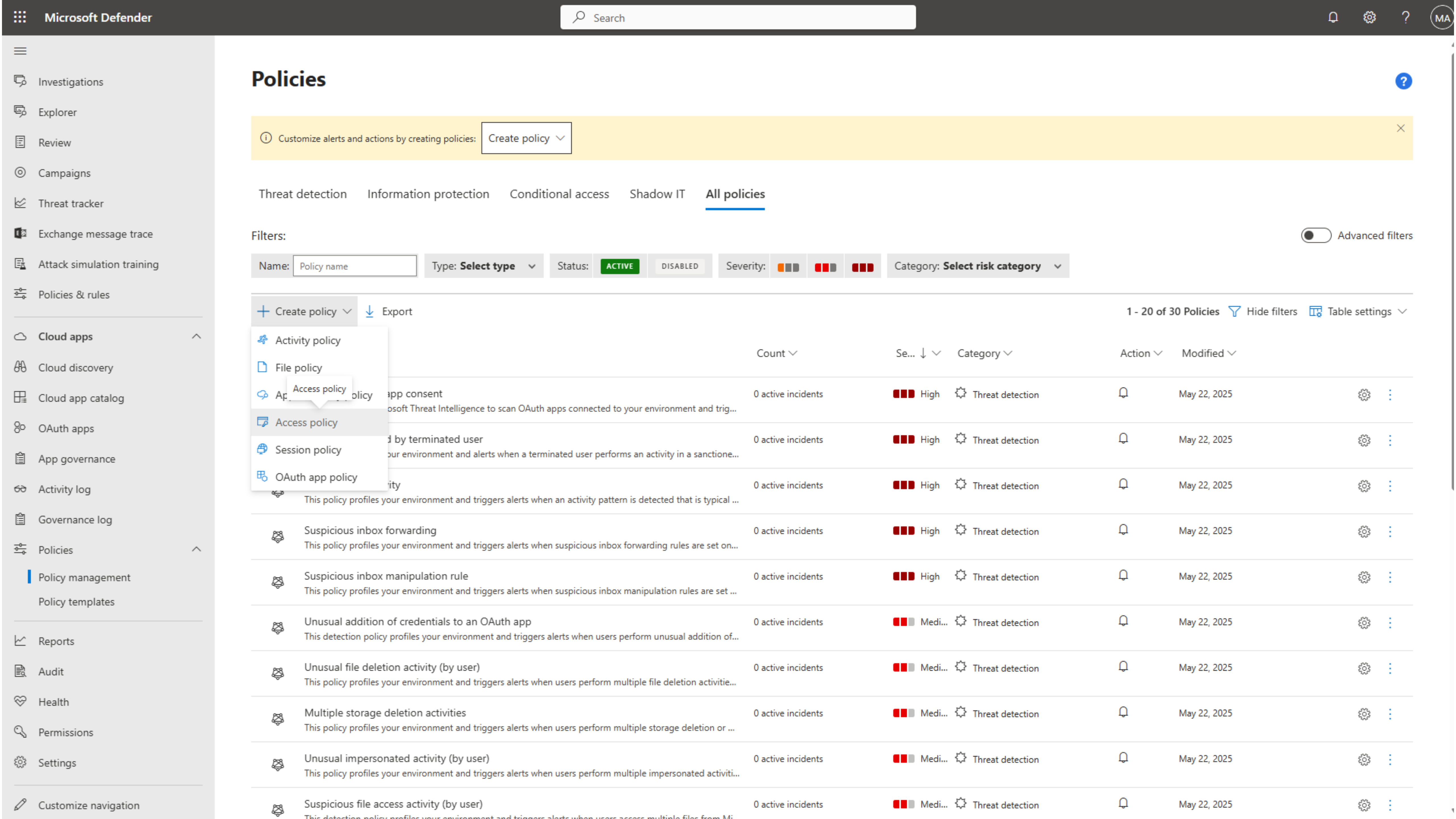
App	Status	Available controls	Was connected on	Last activity
Microsoft 365 Copilot - General Collaboration	✓ Connected	Microsoft Entra conditional ... + Onboard with session c...	May 23, 2025 9:52 AM	May 23, 2025 9:52 AM
Microsoft Exchange Online - General Cloud computing platform	✓ Connected	Microsoft Entra conditional ... Session control	May 23, 2025 9:52 AM	May 23, 2025 9:52 AM
Microsoft Power BI - General Business intelligence	✓ Connected	Microsoft Entra conditional ... Session control	May 23, 2025 9:50 AM	May 23, 2025 9:52 AM
Microsoft Teams - General PREVIEW Online meetings	✓ Connected	Microsoft Entra conditional ... Session control	May 23, 2025 9:52 AM	May 23, 2025 9:52 AM

Custom access policies for Power BI

An access policy created in Defender for Cloud Apps controls whether a user is allowed to sign in to a cloud application like the Power BI service.

Examples to use access policies to **block access to the Power BI service**:

- Unexpected user
- Non-managed device
- Outdated browser or operating system
- Unknown location or IP address



Microsoft Defender

Search

MA

- Investigations
- Explorer
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules
- Cloud apps
- Cloud discovery
- Cloud app catalog
- OAuth apps
- App governance
- Activity log
- Governance log
- Policies
  - Policy management
  - Policy templates
- Reports
- Audit
- Health
- Permissions
- Settings
- Customize navigation

Policies

Customize alerts and actions by creating policies: Create policy

Threat detection | Information protection | Conditional access | Shadow IT | **All policies**

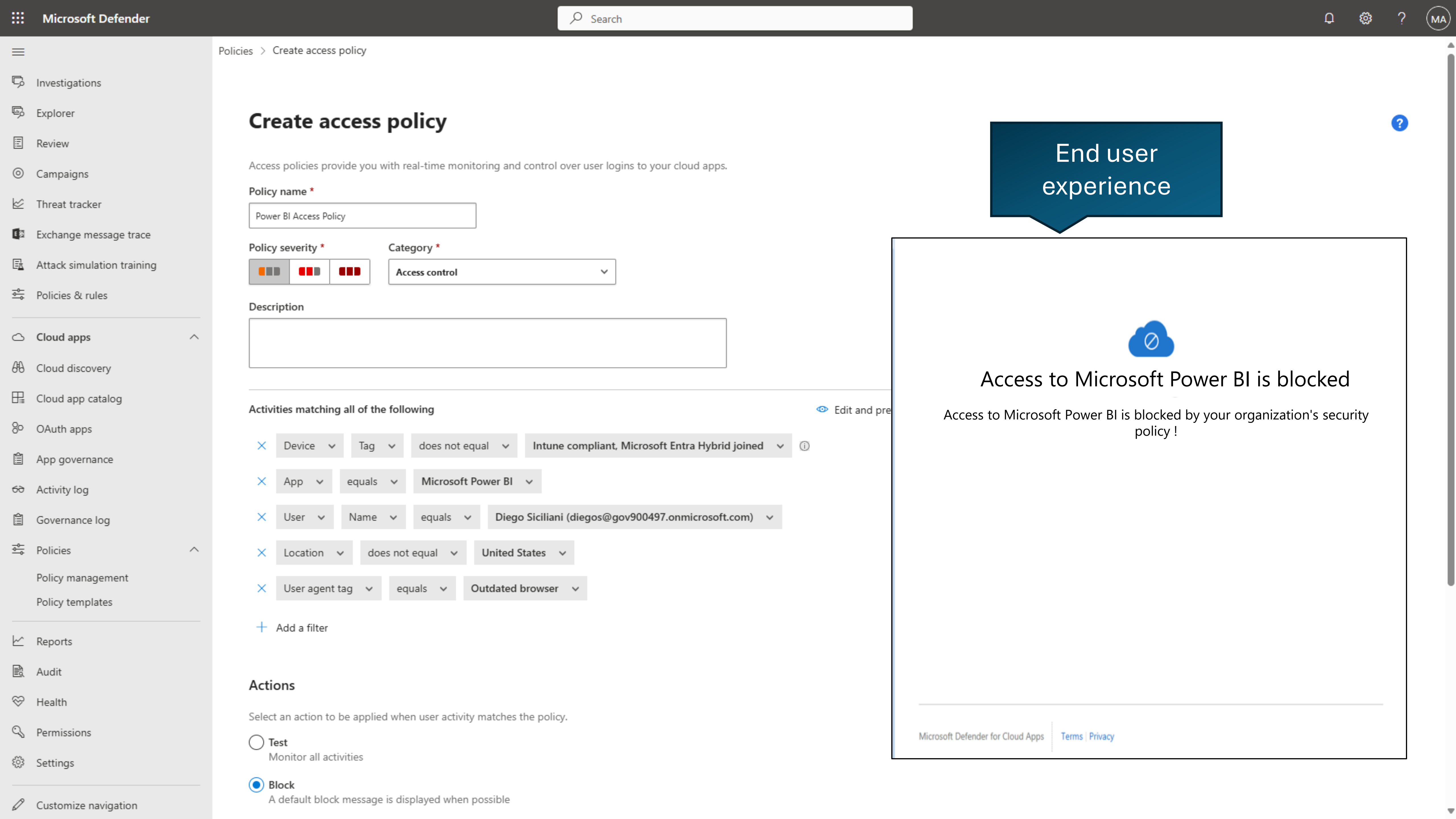
Filters: Advanced filters

Name: Policy name | Type: **Select type** | Status: ACTIVE DISABLED | Severity: | Category: **Select risk category**

+ Create policy | Export | 1 - 20 of 30 Policies | Hide filters | Table settings

- Activity policy
- File policy
- Ap… …olicy (Access policy)
- Access policy
- Session policy
- OAuth app policy

	Count	Se... ↓	Category	Action	Modified
…app consent …osoft Threat Intelligence to scan OAuth apps connected to your environment and trig...	0 active incidents	High	Threat detection		May 22, 2025
…d by terminated user …our environment and alerts when a terminated user performs an activity in a sanctione...	0 active incidents	High	Threat detection		May 22, 2025
…ity This policy profiles your environment and triggers alerts when an activity pattern is detected that is typical ...	0 active incidents	High	Threat detection		May 22, 2025
Suspicious inbox forwarding This policy profiles your environment and triggers alerts when suspicious inbox forwarding rules are set on...	0 active incidents	High	Threat detection		May 22, 2025
Suspicious inbox manipulation rule This policy profiles your environment and triggers alerts when suspicious inbox manipulation rules are set ...	0 active incidents	High	Threat detection		May 22, 2025
Unusual addition of credentials to an OAuth app This detection policy profiles your environment and triggers alerts when users perform unusual addition of...	0 active incidents	Medi...	Threat detection		May 22, 2025
Unusual file deletion activity (by user) This policy profiles your environment and triggers alerts when users perform multiple file deletion activitie...	0 active incidents	Medi...	Threat detection		May 22, 2025
Multiple storage deletion activities This policy profiles your environment and triggers alerts when users perform multiple storage deletion or ...	0 active incidents	Medi...	Threat detection		May 22, 2025
Unusual impersonated activity (by user) This policy profiles your environment and triggers alerts when users perform multiple impersonated activiti...	0 active incidents	Medi...	Threat detection		May 22, 2025
Suspicious file access activity (by user) This detection policy profiles your environment and triggers alerts when users access multiple files from Mi...	0 active incidents	Medi...	Threat detection		May 22, 2025



Create access policy

Access policies provide you with real-time monitoring and control over user logins to your cloud apps.

Policy name *: Power BI Access Policy

Policy severity *: 🟧🟧⬜ | 🟥🟥⬜ | 🟥🟥🟥

Category *: Access control

Description

Activities matching all of the following

Edit and pre

✕	Device	Tag	does not equal	Intune compliant, Microsoft Entra Hybrid joined
✕	App	equals	Microsoft Power BI	
✕	User	Name	equals	Diego Siciliani (diegos@gov900497.onmicrosoft.com)
✕	Location	does not equal	United States	
✕	User agent tag	equals	Outdated browser	

+ Add a filter

Actions

Select an action to be applied when user activity matches the policy.

○ Test
Monitor all activities

● Block
A default block message is displayed when possible

End user experience

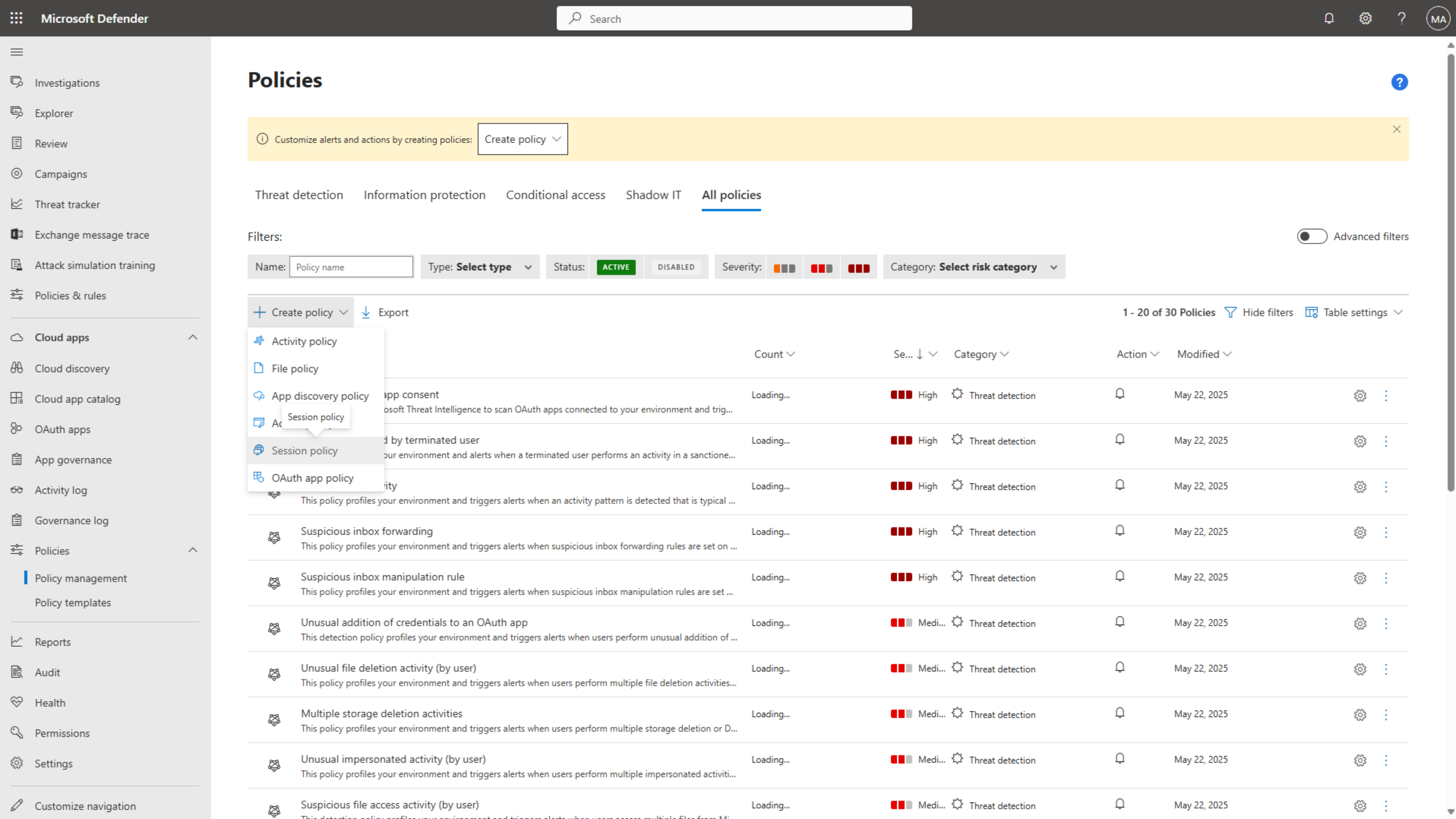
Access to Microsoft Power BI is blocked

Access to Microsoft Power BI is blocked by your organization's security policy !

Custom session policies for Power BI

Use session policies to monitor, block, or control user sessions in the Power BI service. Useful when you don't want to allow or block access completely .

- Example:
  - Block downloads and exports when a specific sensitivity label, like *Highly Restricted*, is assigned to the item in the Power BI service.
  - Monitor when a user, who meets certain conditions, signs in.
  - Control file uploads with session policies



Policies

Customize alerts and actions by creating policies: Create policy

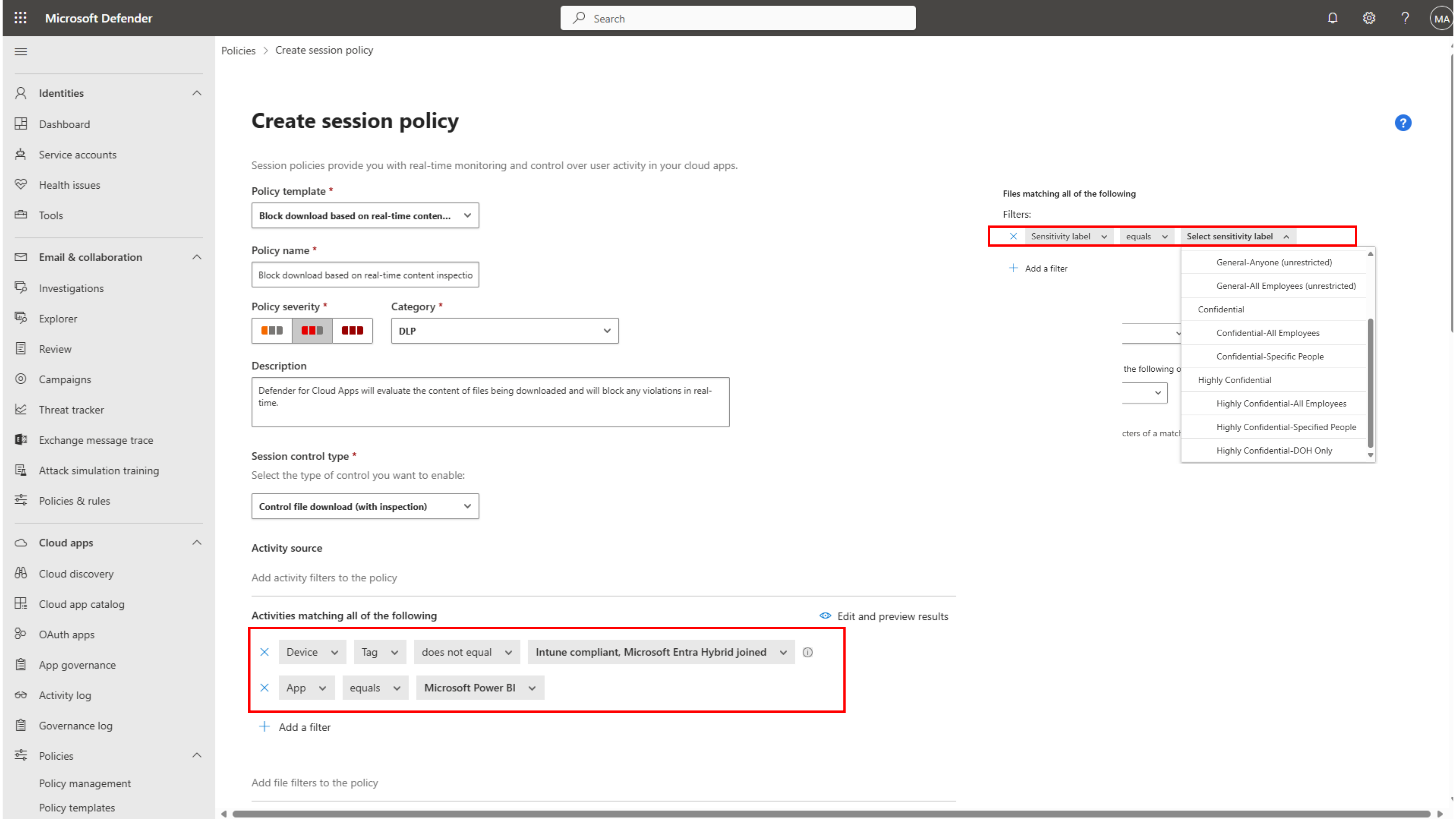
Filters:

Advanced filters

Name: Policy name
Type: **Select type**
Status: ACTIVE DISABLED
Severity:
Category: **Select risk category**

1 - 20 of 30 Policies

	Count	Se... ↓	Category	Action	Modified
app consent osoft Threat Intelligence to scan OAuth apps connected to your environment and trig...	Loading...	High	Threat detection		May 22, 2025
d by terminated user our environment and alerts when a terminated user performs an activity in a sanctione...	Loading...	High	Threat detection		May 22, 2025
ity This policy profiles your environment and triggers alerts when an activity pattern is detected that is typical ...	Loading...	High	Threat detection		May 22, 2025
Suspicious inbox forwarding This policy profiles your environment and triggers alerts when suspicious inbox forwarding rules are set on ...	Loading...	High	Threat detection		May 22, 2025
Suspicious inbox manipulation rule This policy profiles your environment and triggers alerts when suspicious inbox manipulation rules are set ...	Loading...	High	Threat detection		May 22, 2025
Unusual addition of credentials to an OAuth app This detection policy profiles your environment and triggers alerts when users perform unusual addition of ...	Loading...	Medi...	Threat detection		May 22, 2025
Unusual file deletion activity (by user) This policy profiles your environment and triggers alerts when users perform multiple file deletion activities...	Loading...	Medi...	Threat detection		May 22, 2025
Multiple storage deletion activities This policy profiles your environment and triggers alerts when users perform multiple storage deletion or D...	Loading...	Medi...	Threat detection		May 22, 2025
Unusual impersonated activity (by user) This policy profiles your environment and triggers alerts when users perform multiple impersonated activiti...	Loading...	Medi...	Threat detection		May 22, 2025
Suspicious file access activity (by user) This detection policy profiles your environment and triggers alerts when users access multiple files from Mi...	Loading...	Medi...	Threat detection		May 22, 2025



Create session policy

Session policies provide you with real-time monitoring and control over user activity in your cloud apps.

Policy template *
Block download based on real-time conten...

Policy name *
Block download based on real-time content inspectio

Policy severity *

Category *
DLP

Description
Defender for Cloud Apps will evaluate the content of files being downloaded and will block any violations in real-time.

Session control type *
Select the type of control you want to enable:
Control file download (with inspection)

Activity source

Add activity filters to the policy

Activities matching all of the following

Device | Tag | does not equal | Intune compliant, Microsoft Entra Hybrid joined

App | equals | Microsoft Power BI

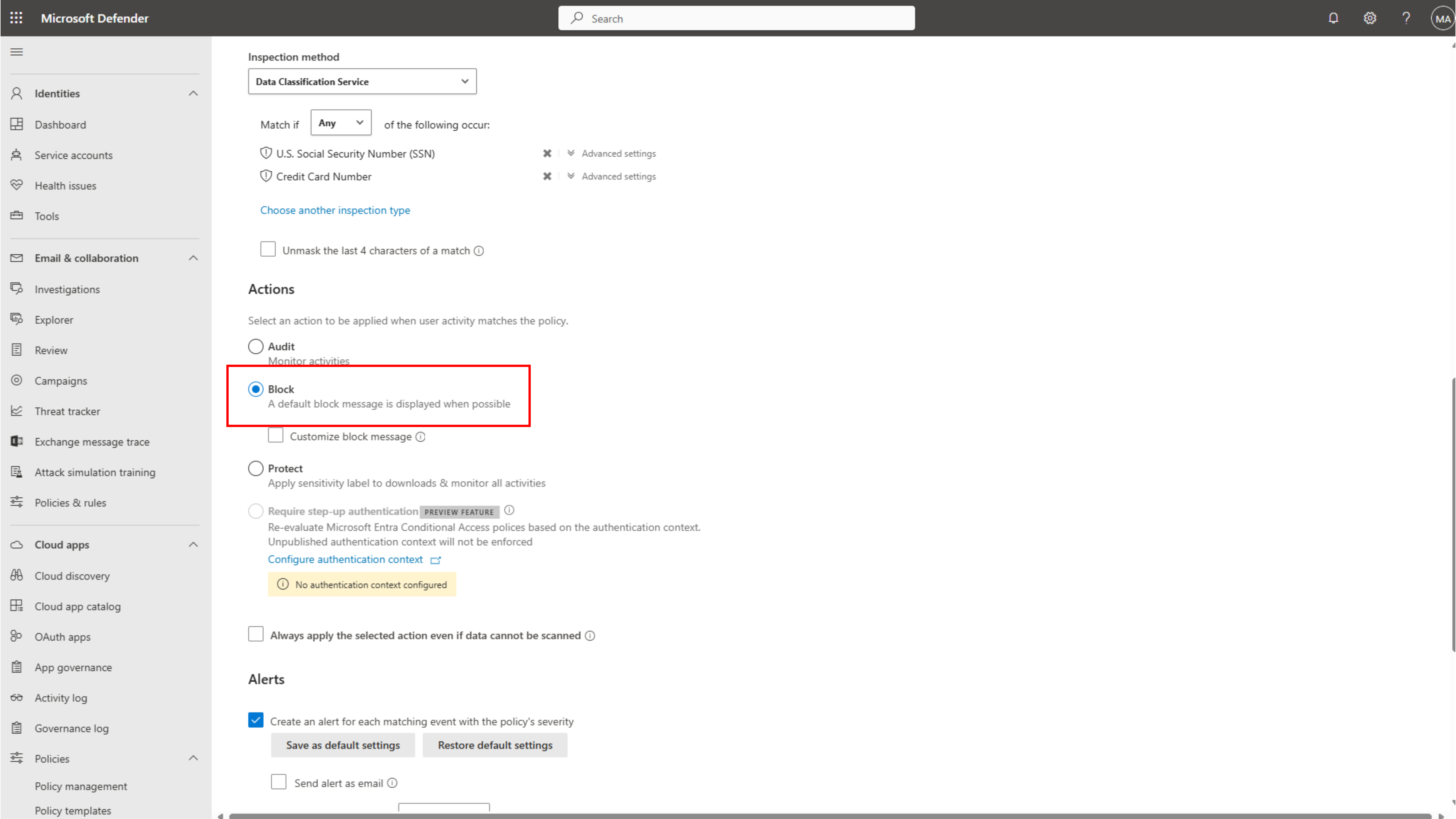
Add file filters to the policy

Files matching all of the following

Filters:

Sensitivity label | equals | Select sensitivity label

General-Anyone (unrestricted)
General-All Employees (unrestricted)
Confidential
Confidential-All Employees
Confidential-Specific People
Highly Confidential
Highly Confidential-All Employees
Highly Confidential-Specified People
Highly Confidential-DOH Only



Inspection method

Data Classification Service

Match if Any of the following occur:

U.S. Social Security Number (SSN) ✖ | Advanced settings

Credit Card Number ✖ | Advanced settings

Choose another inspection type

□ Unmask the last 4 characters of a match ⓘ

Actions

Select an action to be applied when user activity matches the policy.

○ **Audit**
Monitor activities

● **Block**
A default block message is displayed when possible

□ Customize block message ⓘ

○ **Protect**
Apply sensitivity label to downloads & monitor all activities

○ Require step-up authentication PREVIEW FEATURE ⓘ
Re-evaluate Microsoft Entra Conditional Access polices based on the authentication context.
Unpublished authentication context will not be enforced
Configure authentication context

ⓘ No authentication context configured

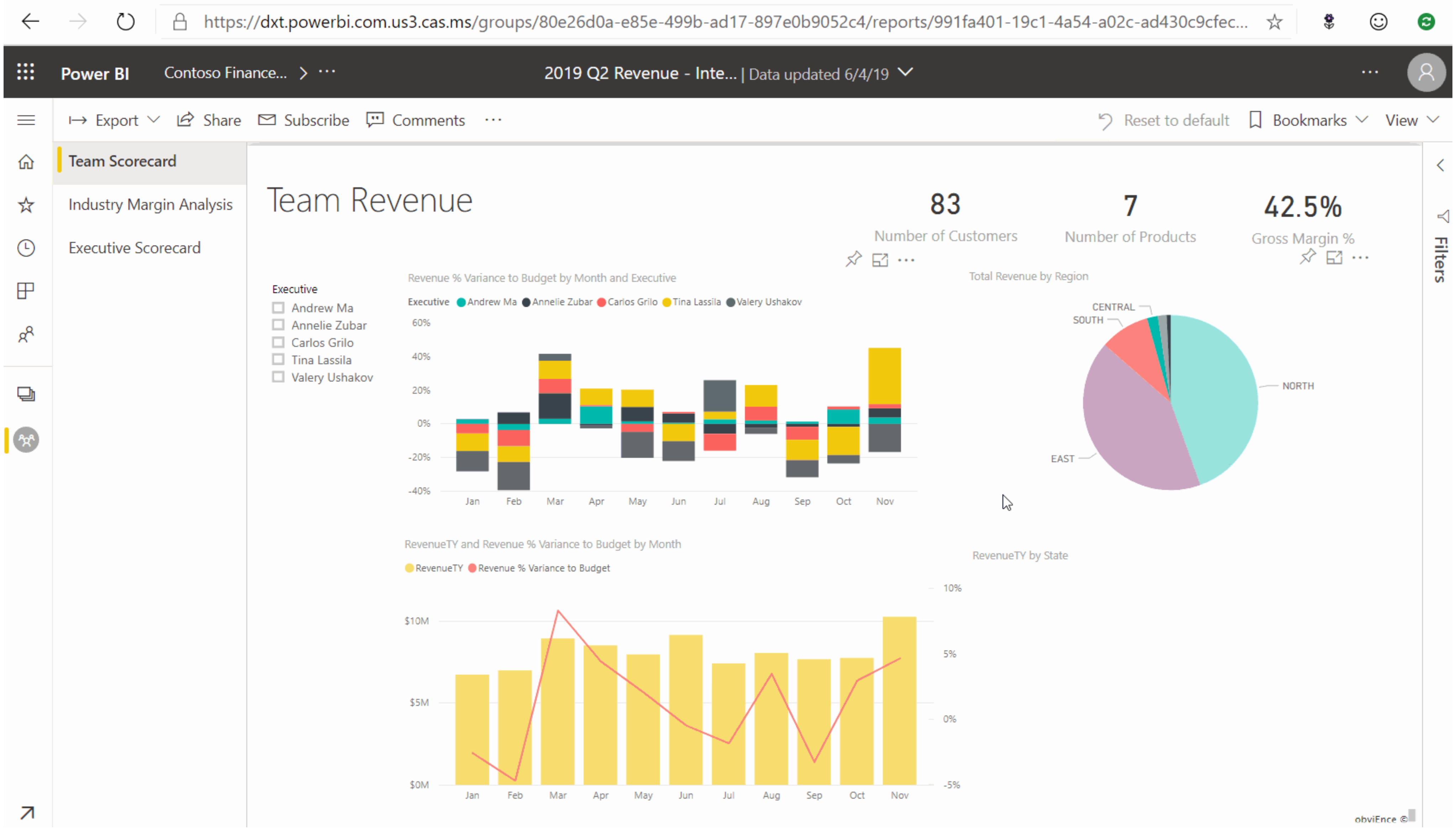
□ **Always apply the selected action even if data cannot be scanned** ⓘ

Alerts

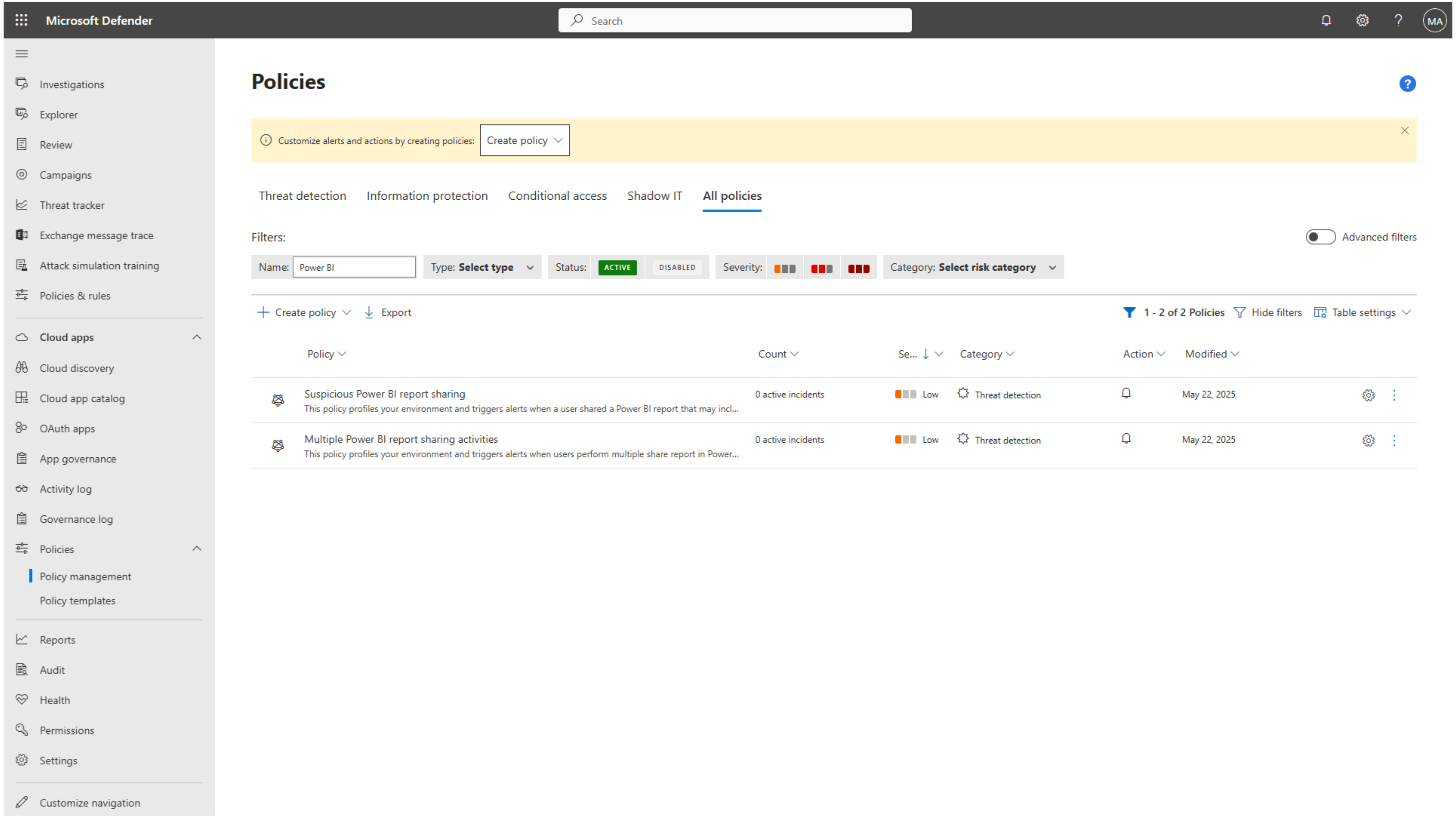
☑ Create an alert for each matching event with the policy's severity

□ Send alert as email ⓘ

Real Time Controls through session policies



Built-in Defender for Cloud Apps detections for Power BI



Microsoft Defender

Search

MA

- Investigations
- Explorer
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules
- Cloud apps
- Cloud discovery
- Cloud app catalog
- OAuth apps
- App governance
- Activity log
- Governance log
- Policies
- Policy management
- Policy templates
- Reports
- Audit
- Health
- Permissions
- Settings
- Customize navigation

Policies

Customize alerts and actions by creating policies: Create policy

Threat detection | Information protection | Conditional access | Shadow IT | **All policies**

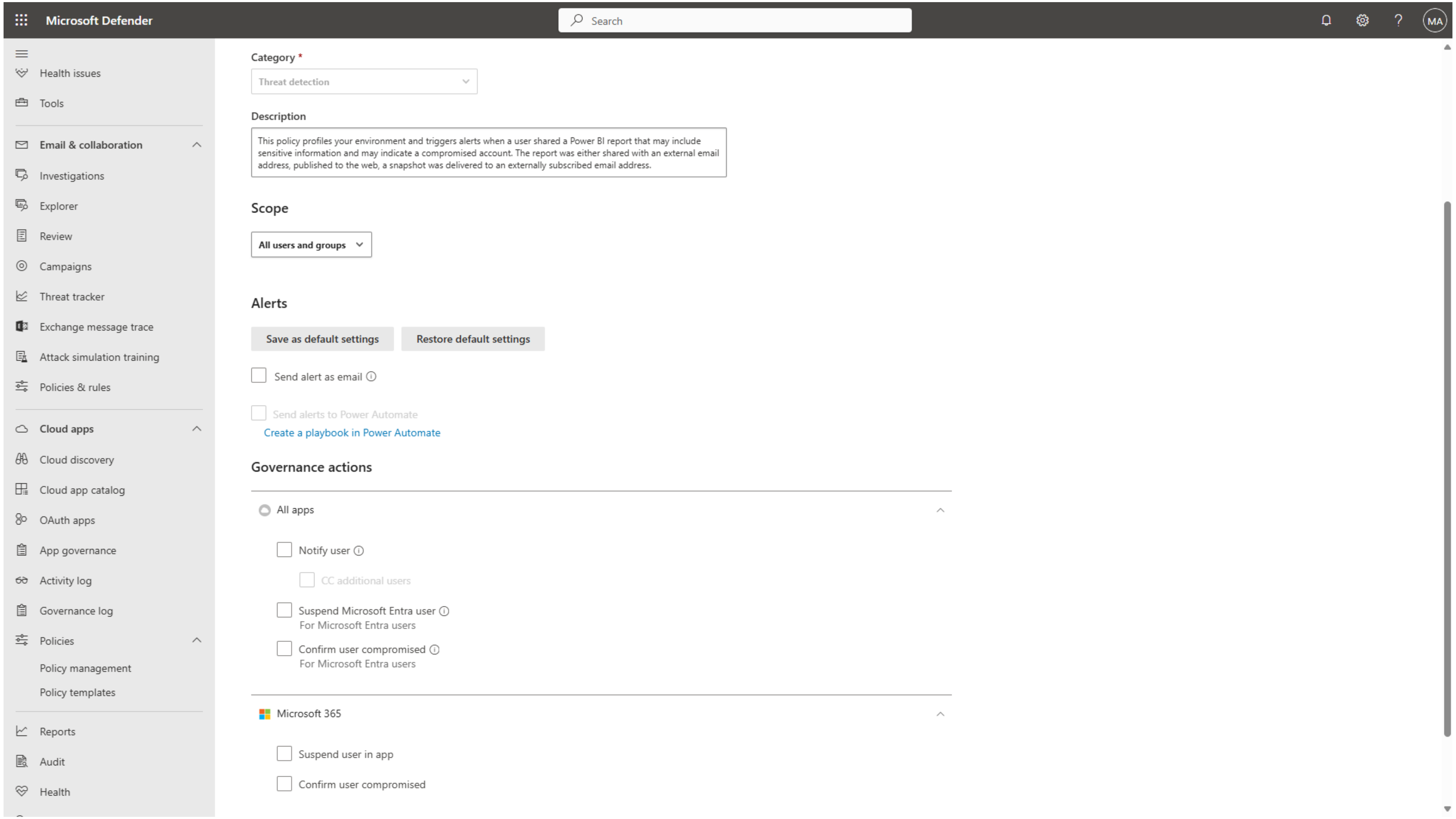
Filters: Name: Power BI | Type: **Select type** | Status: ACTIVE DISABLED | Severity: | Category: **Select risk category**

Advanced filters

+ Create policy | Export | 1 - 2 of 2 Policies | Hide filters | Table settings

Policy	Count	Se...	Category	Action	Modified
Suspicious Power BI report sharing This policy profiles your environment and triggers alerts when a user shared a Power BI report that may incl...	0 active incidents	Low	Threat detection		May 22, 2025
Multiple Power BI report sharing activities This policy profiles your environment and triggers alerts when users perform multiple share report in Power...	0 active incidents	Low	Threat detection		May 22, 2025

Set anomaly detection policies to monitor Power BI activities



Category *

Threat detection

Description

This policy profiles your environment and triggers alerts when a user shared a Power BI report that may include sensitive information and may indicate a compromised account. The report was either shared with an external email address, published to the web, a snapshot was delivered to an externally subscribed email address.

Scope

All users and groups

Alerts

Save as default settings | Restore default settings

□ Send alert as email ⓘ

□ Send alerts to Power Automate

Create a playbook in Power Automate

Governance actions

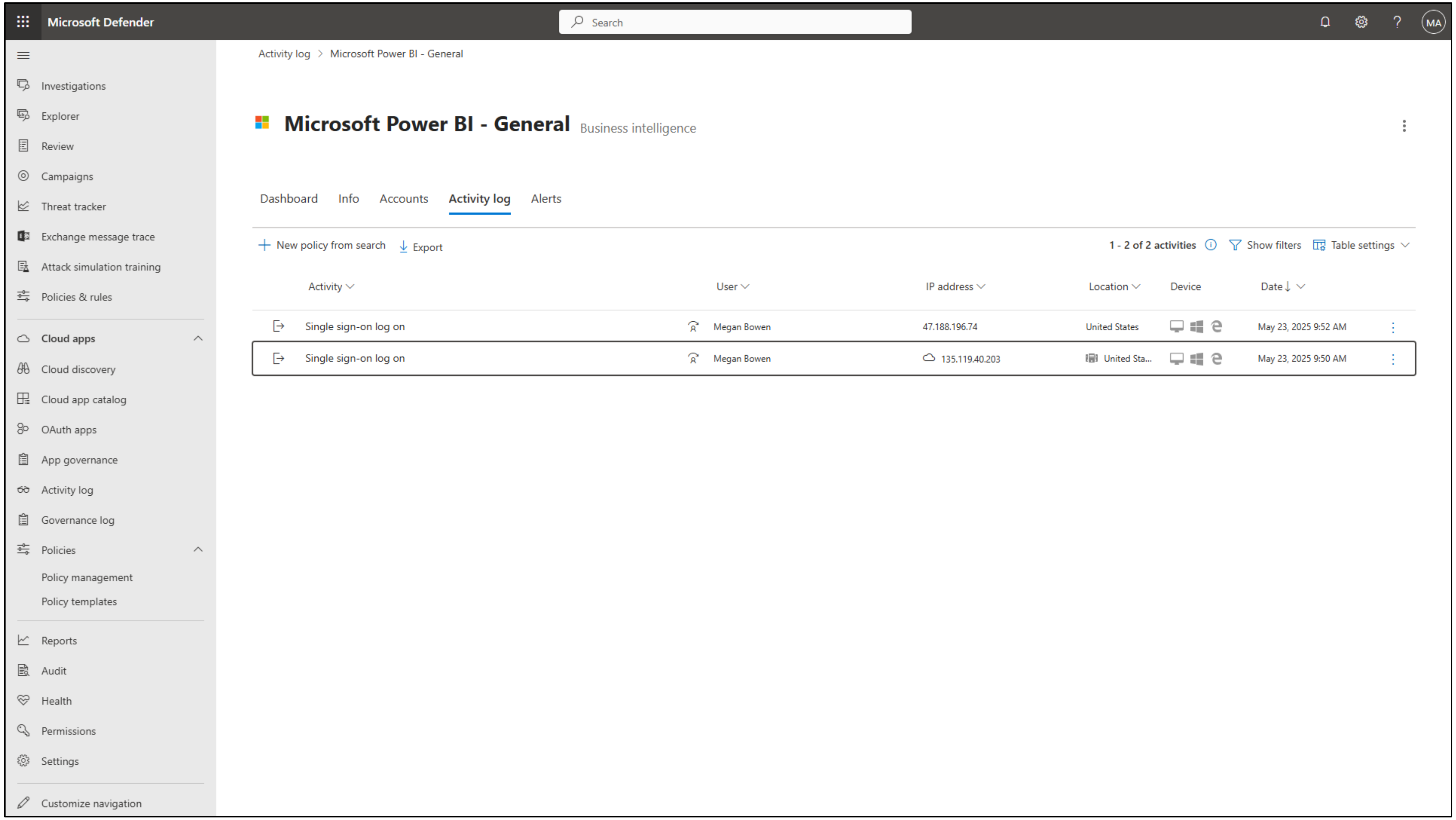
○ All apps

- □ Notify user ⓘ
  - □ CC additional users
- □ Suspend Microsoft Entra user ⓘ
  For Microsoft Entra users
- □ Confirm user compromised ⓘ
  For Microsoft Entra users

Microsoft 365

- □ Suspend user in app
- □ Confirm user compromised

Defender for Cloud Apps - Activity Log for Power BI

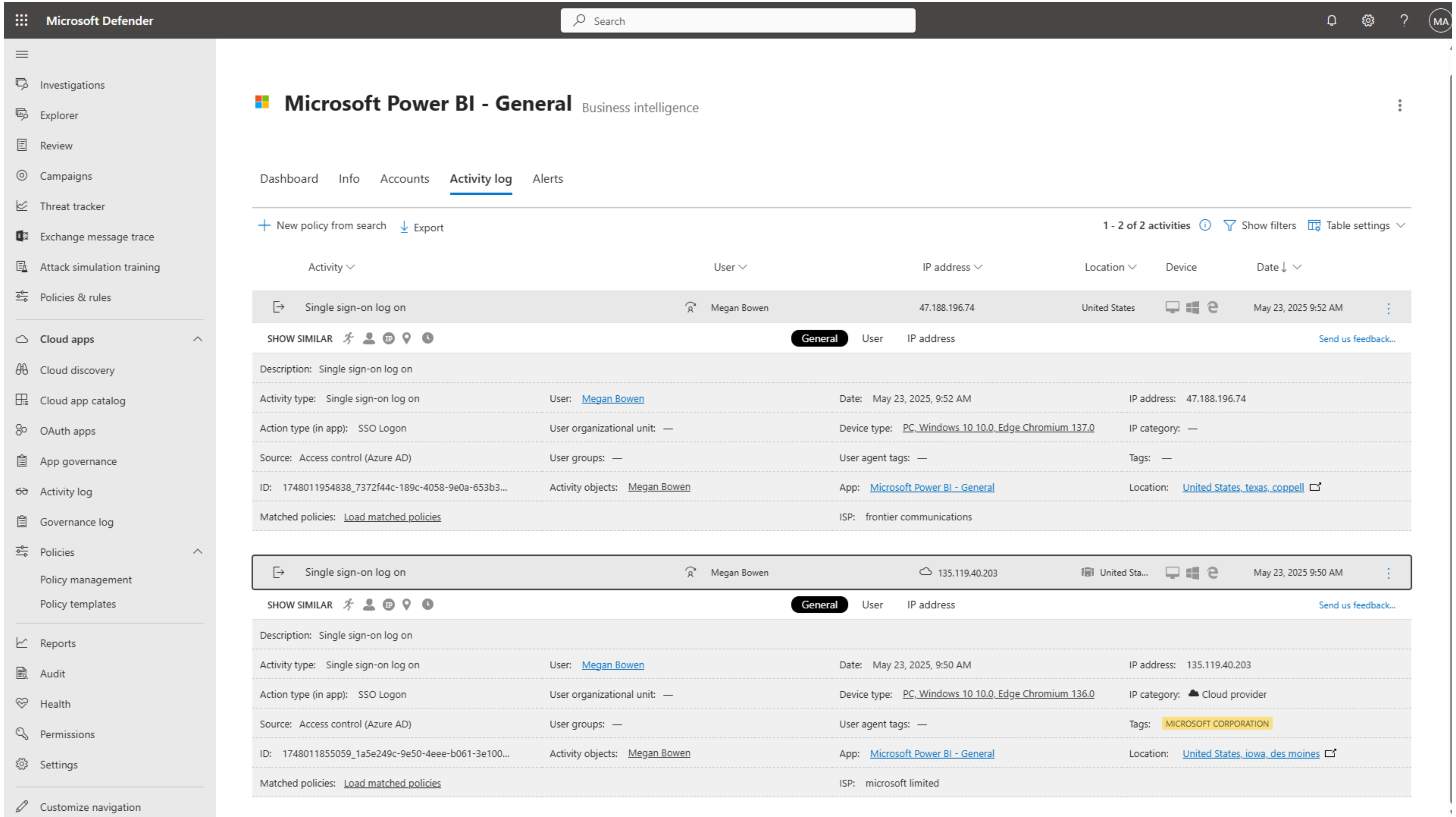


Microsoft Power BI - General Business intelligence

1 - 2 of 2 activities

Activity	User	IP address	Location	Device	Date
Single sign-on log on	Megan Bowen	47.188.196.74	United States		May 23, 2025 9:52 AM
Single sign-on log on	Megan Bowen	135.119.40.203	United Sta...		May 23, 2025 9:50 AM

Defender for Cloud Apps -Activity Log for Power BI



Microsoft Power BI - General Business intelligence

1 - 2 of 2 activities

Activity	User	IP address	Location	Device	Date ↓
Single sign-on log on	Megan Bowen	47.188.196.74	United States		May 23, 2025 9:52 AM
Single sign-on log on	Megan Bowen	135.119.40.203	United Sta...		May 23, 2025 9:50 AM

Description: Single sign-on log on

Activity type: Single sign-on log on
User: Megan Bowen
Date: May 23, 2025, 9:52 AM
IP address: 47.188.196.74

Action type (in app): SSO Logon
User organizational unit: —
Device type: PC, Windows 10 10.0, Edge Chromium 137.0
IP category: —

Source: Access control (Azure AD)
User groups: —
User agent tags: —
Tags: —

ID: 1748011954838_7372f44c-189c-4058-9e0a-653b3...
Activity objects: Megan Bowen
App: Microsoft Power BI - General
Location: United States, texas, coppell

Matched policies: Load matched policies
ISP: frontier communications

Description: Single sign-on log on

Activity type: Single sign-on log on
User: Megan Bowen
Date: May 23, 2025, 9:50 AM
IP address: 135.119.40.203

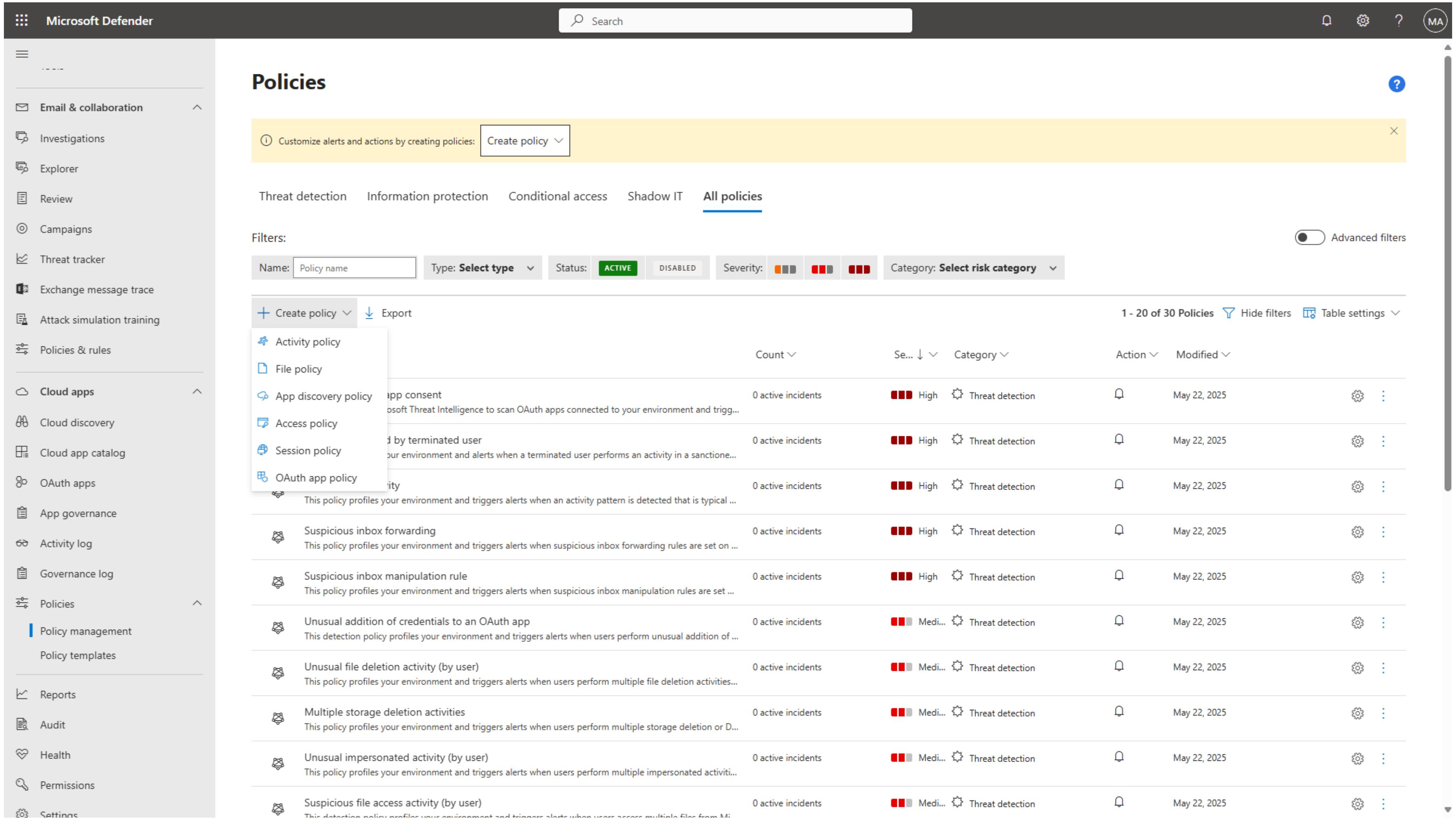
Action type (in app): SSO Logon
User organizational unit: —
Device type: PC, Windows 10 10.0, Edge Chromium 136.0
IP category: Cloud provider

Source: Access control (Azure AD)
User groups: —
User agent tags: —
Tags: MICROSOFT CORPORATION

ID: 1748011855059_1a5e249c-9e50-4eee-b061-3e100...
Activity objects: Megan Bowen
App: Microsoft Power BI - General
Location: United States, iowa, des moines

Matched policies: Load matched policies
ISP: microsoft limited

Custom policies to alert on suspicious user activity in Power BI



Policies

Customize alerts and actions by creating policies: Create policy

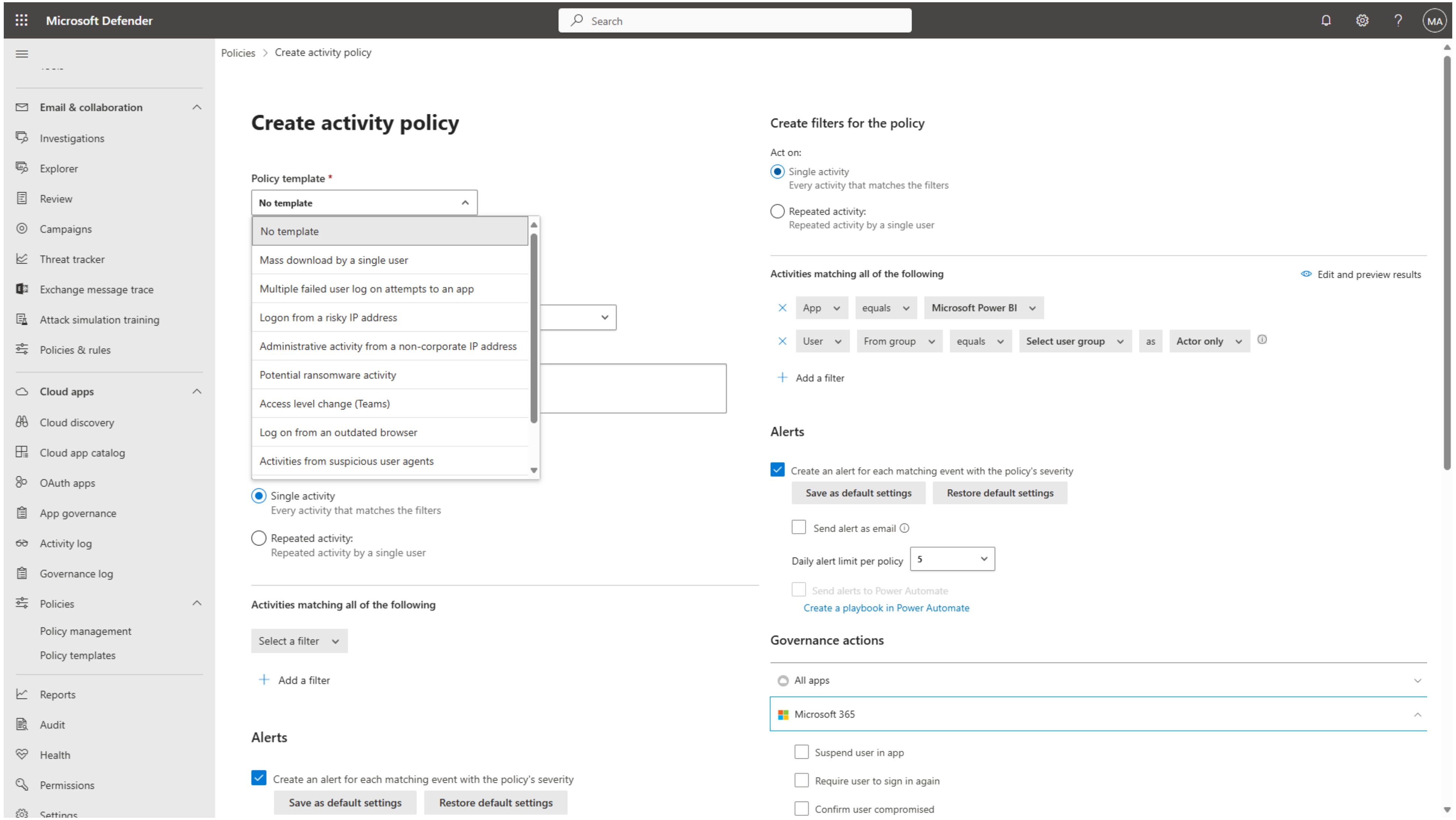
Filters:

Name: Policy name | Type: Select type | Status: ACTIVE DISABLED | Severity: | Category: Select risk category

1 - 20 of 30 Policies

	Count	Se... ↓	Category	Action	Modified
app consent osoft Threat Intelligence to scan OAuth apps connected to your environment and trigg...	0 active incidents	High	Threat detection	🔔	May 22, 2025
d by terminated user our environment and alerts when a terminated user performs an activity in a sanctione...	0 active incidents	High	Threat detection	🔔	May 22, 2025
ity This policy profiles your environment and triggers alerts when an activity pattern is detected that is typical ...	0 active incidents	High	Threat detection	🔔	May 22, 2025
Suspicious inbox forwarding This policy profiles your environment and triggers alerts when suspicious inbox forwarding rules are set on ...	0 active incidents	High	Threat detection	🔔	May 22, 2025
Suspicious inbox manipulation rule This policy profiles your environment and triggers alerts when suspicious inbox manipulation rules are set ...	0 active incidents	High	Threat detection	🔔	May 22, 2025
Unusual addition of credentials to an OAuth app This detection policy profiles your environment and triggers alerts when users perform unusual addition of ...	0 active incidents	Medi...	Threat detection	🔔	May 22, 2025
Unusual file deletion activity (by user) This policy profiles your environment and triggers alerts when users perform multiple file deletion activities...	0 active incidents	Medi...	Threat detection	🔔	May 22, 2025
Multiple storage deletion activities This policy profiles your environment and triggers alerts when users perform multiple storage deletion or D...	0 active incidents	Medi...	Threat detection	🔔	May 22, 2025
Unusual impersonated activity (by user) This policy profiles your environment and triggers alerts when users perform multiple impersonated activiti...	0 active incidents	Medi...	Threat detection	🔔	May 22, 2025
Suspicious file access activity (by user) This detection policy profiles your environment and triggers alerts when users access multiple files from Mi	0 active incidents	Medi...	Threat detection	🔔	May 22, 2025

Custom policies to alert on suspicious user activity in Power BI



Policies > Create activity policy

Create activity policy

Policy template *

No template

- No template
- Mass download by a single user
- Multiple failed user log on attempts to an app
- Logon from a risky IP address
- Administrative activity from a non-corporate IP address
- Potential ransomware activity
- Access level change (Teams)
- Log on from an outdated browser
- Activities from suspicious user agents

● Single activity
Every activity that matches the filters

○ Repeated activity:
Repeated activity by a single user

Activities matching all of the following

Select a filter

+ Add a filter

Alerts

☑ Create an alert for each matching event with the policy's severity

Save as default settings | Restore default settings

Create filters for the policy

Act on:

● Single activity
Every activity that matches the filters

○ Repeated activity:
Repeated activity by a single user

Activities matching all of the following | Edit and preview results

✕ App | equals | Microsoft Power BI

✕ User | From group | equals | Select user group | as | Actor only

+ Add a filter

Alerts

☑ Create an alert for each matching event with the policy's severity

Save as default settings | Restore default settings

☐ Send alert as email

Daily alert limit per policy: 5

☐ Send alerts to Power Automate

Create a playbook in Power Automate

Governance actions

All apps

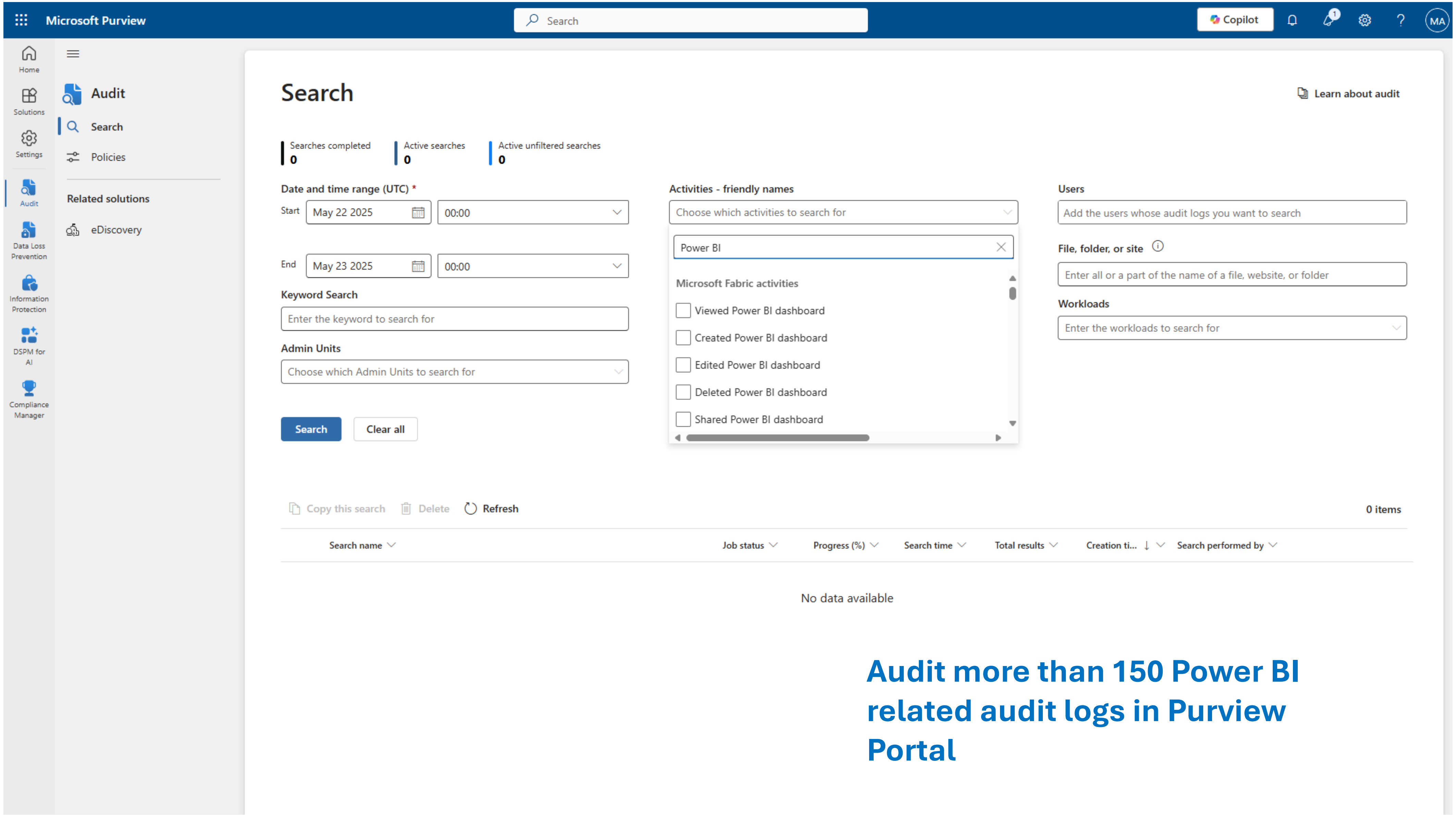
Microsoft 365

☐ Suspend user in app

☐ Require user to sign in again

☐ Confirm user compromised

Power BI Audit logs in Microsoft Purview



Search

Searches completed 0
Active searches 0
Active unfiltered searches 0

Date and time range (UTC) *
Start May 22 2025 00:00
End May 23 2025 00:00

Keyword Search
Enter the keyword to search for

Admin Units
Choose which Admin Units to search for

Search
Clear all

Activities - friendly names
Choose which activities to search for
Power BI
Microsoft Fabric activities
□ Viewed Power BI dashboard
□ Created Power BI dashboard
□ Edited Power BI dashboard
□ Deleted Power BI dashboard
□ Shared Power BI dashboard

Users
Add the users whose audit logs you want to search

File, folder, or site
Enter all or a part of the name of a file, website, or folder

Workloads
Enter the workloads to search for

Copy this search | Delete | Refresh | 0 items

Search name	Job status	Progress (%)	Search time	Total results	Creation ti... ↓	Search performed by

No data available

Audit more than 150 Power BI related audit logs in Purview Portal

Power BI Security Licenses for GCC

Feature	Required Licenses
Sensitivity Labels	Power BI Pro OR Premium Per User (PPU) + M365 G3/AIP P2/M365 G5 IP&G/M365 G5 Compliance/G5 licenses
DLP Policies	Power BI Premium capacity OR Premium Per User (PPU) + M365 G5 IP&G/M365 G5 Compliance/M365 G5 licenses
Security Monitoring	M365 G5 IP&G/M365 G5 Compliance/M365 G5 licenses
Audit Log Retention (1 year)	M365G5 eDiscovery & Audit /M365 G5 Compliance/M365 G5 licenses

Additional Info

- **References**:
  - Info Protection and DLP for Power BI
  - Sensitivity labels in Power BI
  - Defender for Cloud Apps for Power BI
  - Auditing of information protection and data loss prevention for Power BI

- **Next Session** – Guidance on CJIS Compliance for State and Government agencies.

- Schedule a meeting with a SLG Purview Specialist for any questions or live demonstrations. Email: MSSLGCompliance@microsoft.com

Questions