

Manage Workspaces

AI & Data Analytics



Create and manage workspaces and assets

- Create and configure a **workspace**
- Configure and update a workspace app
- Publish, import, or update items in a workspace
- Create **dashboards**
- Choose a **distribution** method
- Configure **subscriptions** and **data alerts**
- **Promote** or **certify** Power BI content
- Identify when a **gateway** is required
- Configure a semantic **model scheduled refresh**



Publish as app

To distribute your dashboard to a broad audience (*many many people*) in your organization, **publish** them as an **app**, either to a group or to your whole organization.

- For your users to view your app, they need a **Power BI Pro license**, too, or the app needs to be stored in a **Power BI Premium** capacity.
- You can publish apps to people outside your organization, too. They can view and interact with the app content, but can't share it with others.



Subscribe _{vs} Data alert Promote _{vs} Certify



Subscribe to report or dashboard

- When you subscribe, you receive an **email** on a **schedule** you set.
- The email contains a **snapshot** and link to the **report or dashboard** or a **full attachment** of the report or dashboard.

Subscriptions



Keep track of your data by subscribing to this report.

The sensitivity label on this report does not appear in emails.

[Manage all](#)

▼ Sales analysis



Subscription name *

Sales analysis

Recipients *

Zala...

Enter email addresses

Attach full report

None

Scheduled date and time

Start date *

6/23/2023



End date

M/d/yyyy



Repeat *

Daily

Scheduled time *

1



15



AM



Time zone *

(UTC-05:00) Eastern Time (US and Canada)



Emails will be sent daily at 01:15 AM Eastern Standard Time starting Friday, June 23, 2023.

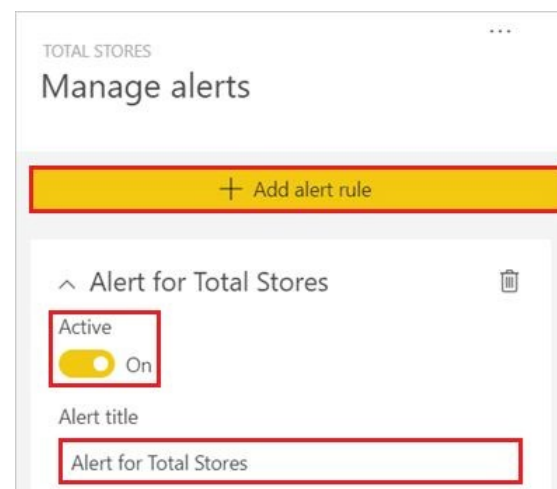
> More options

Save

New subscription

Data alert

- Data alerts notify you when data in your dashboards changes beyond the **threshold** you set.
- Set alerts on tiles in your Workspace
- Only on **gauges, KPIs, and cards**



Condition

Threshold

Above

▼

100

Maximum notification frequency

☒ At most every 24 hours
 ☐ At most once an hour

Alerts are only sent if your data changes.

By default, you'll receive notifications on the service in the notification center.

☒ Send me email, too

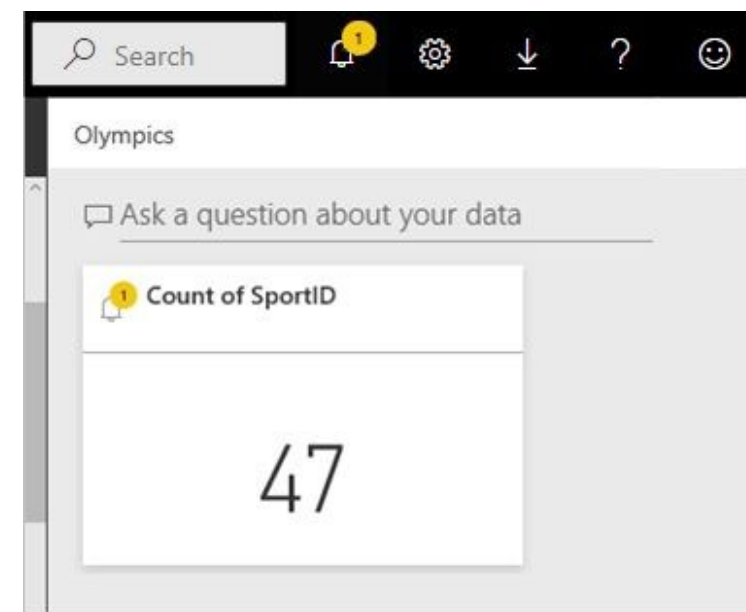
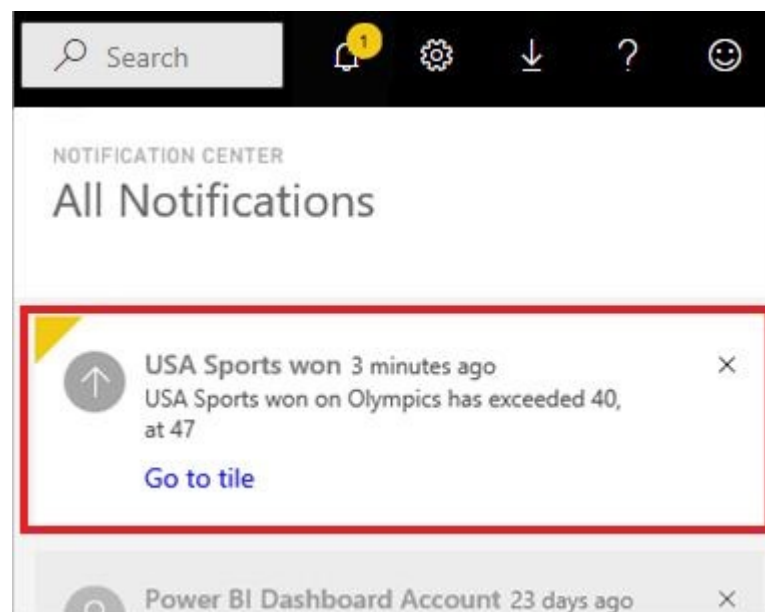
[Use Microsoft Power Automate to trigger additional actions](#)

Save and close

Cancel

Data alert

- Power BI sends an alert to your **Notification center** and, optionally, an email.
- Each alert contains a direct link to your data. Select the link to see the relevant tile



Endorse your content

Power BI provides two ways you can endorse your content to increase its visibility:

1. Promote

- **highlight content** you think is valuable and worthwhile for others to use.
- encourages the collaborative use and spread of content within an organization.
- *Who* can do it: Content owner or workspace member

2. Certify

- content meets the organization's quality standards and can be regarded as **reliable**, authoritative, and ready for use across the organization.
- *Who* can do it: Authorized reviewers (defined by Power BI administrator)

Secure and govern Power BI items

- Assign **workspace roles**
- Configure **item-level access**
- Configure **access** to **semantic models**
- Implement **row-level security** security roles
- Configure **row-level security** group membership
- Apply **sensitivity labels**



Assign Workspace Roles



Collaborate with co-workers

Collaborate with coworkers in **workspaces** to create meaningful reports and dashboards.

In Power BI workspaces, teams share the ownership and management of their

- Dashboards
- Reports
- semantic models
- workbooks.

Workspace Roles

Workspaces provide **roles** that determine what permissions coworkers have.

- Admin
- Member
- Contributor
- Viewer

Capability	Admin	Member	Contributor	Viewer
Delete the workspace	✓	✗	✗	✗
Add admins	✓	✗	✗	✗
Add members	✓	✓	✗	✗
Write data	✓	✓	✓	✗
Create items	✓	✓	✓	✗
Read data	✓	✓	✓	✓

1

Workspace Role:
Admin

Admin

- **Workspace** permissions
 - Update and delete workspace
 - Add/remove workspace users

Capability	Admin	Member	Contributor	Viewer
Update and delete the workspace.	✓			
Add or remove any user in a workspace role.	✓			
Allow Contributors to update the app for the workspace.	✓			
Add members or others with lower permissions.	✓	✓		
Publish, unpublish, and change permissions for an app.	✓	✓		
Update an app.	✓	✓	If allowed ¹	
Share items in apps, including semantic models. ²	✓	✓		
Allow others to reshare items. ²	✓	✓		
Feature apps on colleagues' home. ⁷	✓	✓		
Manage semantic model permissions. ³	✓	✓		
Feature dashboards and reports on colleagues' home. ⁶	✓	✓	✓	

Workspace Role: **2 Member**

Member

- Add members, contributors, viewers
- **App** permissions
 - Publish/unpublish app
 - Feature app
- **Item** permissions
 - Share items
 - Manage semantic model permissions

Whatever **Member** can do, **Admin** also have the rights.

Capability	Admin	Member	Contributor	Viewer
Update and delete the workspace.	✓			
Add or remove any user in a workspace role.	✓			
Allow Contributors to update the app for the workspace.	✓			
Add members or others with lower permissions.	✓	✓		
Publish, unpublish, and change permissions for an app.	✓	✓		
Update an app.	✓	✓	If allowed ¹	
Share items in apps, including semantic models. ²	✓	✓		
Allow others to reshare items. ²	✓	✓		
Feature apps on colleagues' home. ⁷	✓	✓		
Manage semantic model permissions. ³	✓	✓		
Feature dashboards and reports on colleagues' home. ⁶	✓	✓	✓	

Workspace Role: 3 Contributor

Contributor

- **Report** permissions
 - Modify contents such as reports
 - Create and copy reports
 - Feature reports
 - Subscribe other users to reports

Whatever **Contributor** can do, **Member** and **Admin** also have the rights.

Capability	Admin	Member	Contributor	Viewer
Publish, Create, edit, and delete content, such as reports, in the workspace.	✓	✓	✓	
Create a report in another workspace based on a semantic model in this workspace. ³	✓	✓	✓	
Copy a report. ³	✓	✓	✓	
Create metrics that's based on a semantic model in the workspace. ³	✓	✓	✓	
Schedule data refreshes via the on-premises gateway. ⁴	✓	✓	✓	
Modify gateway connection settings. ⁴	✓	✓	✓	
View and interact with an item. ⁵	✓	✓	✓	✓
Read data that's stored in workspace dataflows.	✓	✓	✓	✓
Create subscriptions to reports ⁶	✓	✓	✓	✓
Subscribe others to reports ⁶	✓	✓	✓	
Manage subscriptions created by others.	✓			
Can receive subscriptions created by others ⁶		✓	✓	✓

Workspace Role: 4 Viewer

Viewer

- Read-only access
- Can interact with items in Workspace
- Create and receive subscriptions

Whatever **Viewer** can do, **Contributor**, **Member** and **Admin** also have the rights.


Capability	Admin	Member	Contributor	Viewer
Publish, Create, edit, and delete content, such as reports, in the workspace.	✓	✓	✓	
Create a report in another workspace based on a semantic model in this workspace. ³	✓	✓	✓	
Copy a report. ³	✓	✓	✓	
Create metrics that's based on a semantic model in the workspace. ³	✓	✓	✓	
Schedule data refreshes via the on-premises gateway. ⁴	✓	✓	✓	
Modify gateway connection settings. ⁴	✓	✓	✓	
View and interact with an item. ⁵	✓	✓	✓	✓
Read data that's stored in workspace dataflows.	✓	✓	✓	✓
Create subscriptions to reports ⁶	✓	✓	✓	✓
Subscribe others to reports ⁶	✓	✓	✓	
Manage subscriptions created by others.	✓			
Can receive subscriptions created by others ⁶		✓	✓	✓

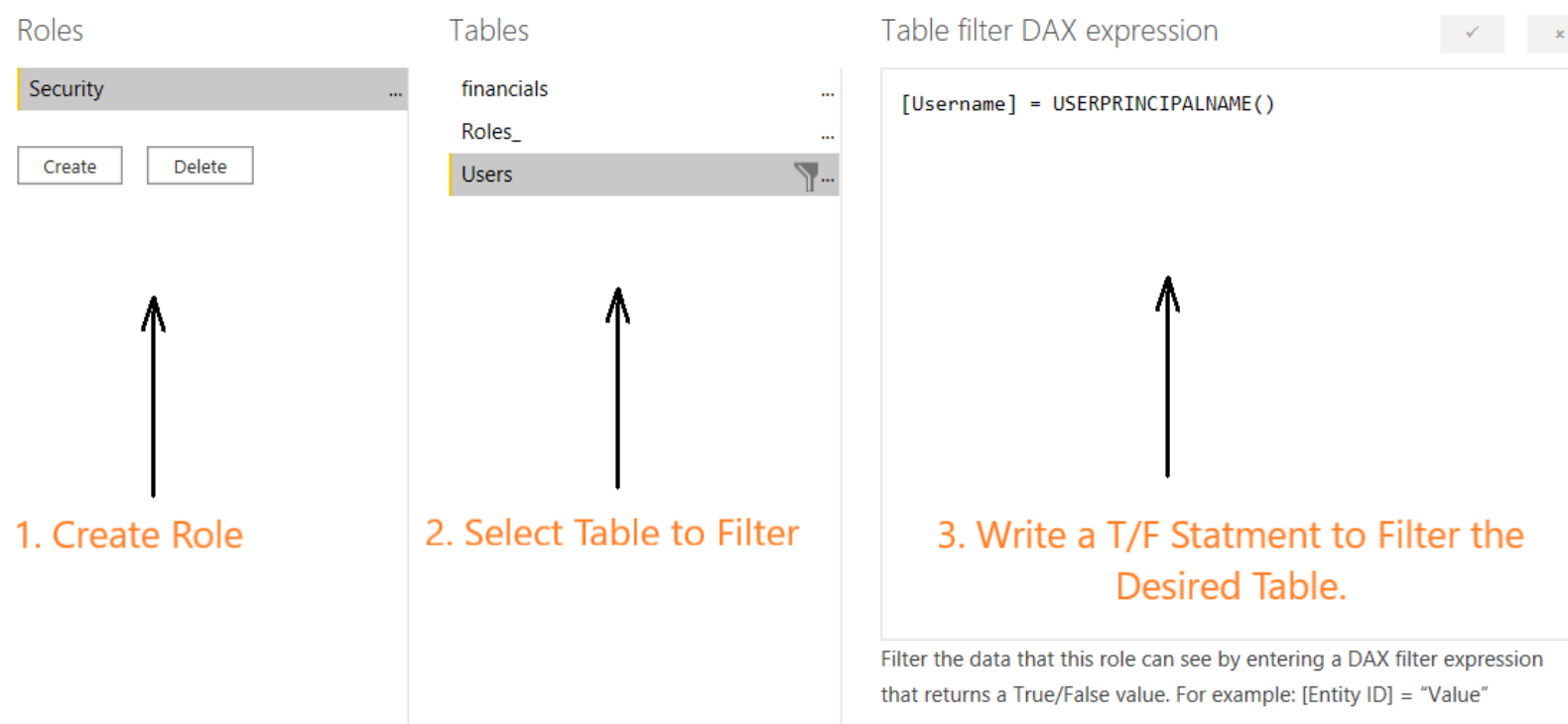


Row-level Security (RLS)



Row-level Security (RLS)

- **Row-level security (RLS)** with Power BI can be used to **restrict data access** for given users.
- RLS only restricts data access for users with **Viewer** permissions. It doesn't apply to Admins,  [Manage roles](#)



The screenshot displays the 'Manage roles' interface in Power BI. It is divided into three main sections: 'Roles', 'Tables', and 'Table filter DAX expression'.

- Roles:** Shows a list of roles with 'Security' selected. Below the list are 'Create' and 'Delete' buttons. An arrow points to this section with the instruction: **1. Create Role**.
- Tables:** Shows a list of tables including 'financials', 'Roles_', and 'Users'. The 'Users' table is selected. An arrow points to this section with the instruction: **2. Select Table to Filter**.
- Table filter DAX expression:** A text box containing the DAX expression `[Username] = USERPRINCIPALNAME()`. An arrow points to this section with the instruction: **3. Write a T/F Statment to Filter the Desired Table.**

Below the DAX expression box, there is a note: "Filter the data that this role can see by entering a DAX filter expression that returns a True/False value. For example: [Entity ID] = 'Value'" data-bbox="538 868 800 908"/>

RLS Use Cases

1. Employee Based RLS

- Users see information that they are tied to or responsible for (Email/ Name)

2. Business Line Based RLS

- Users should only see information within a specific business line (Product/Service/Department).

Table filter DAX expression

☒
☐

```
[Region] = "East"
```

Row-level Security

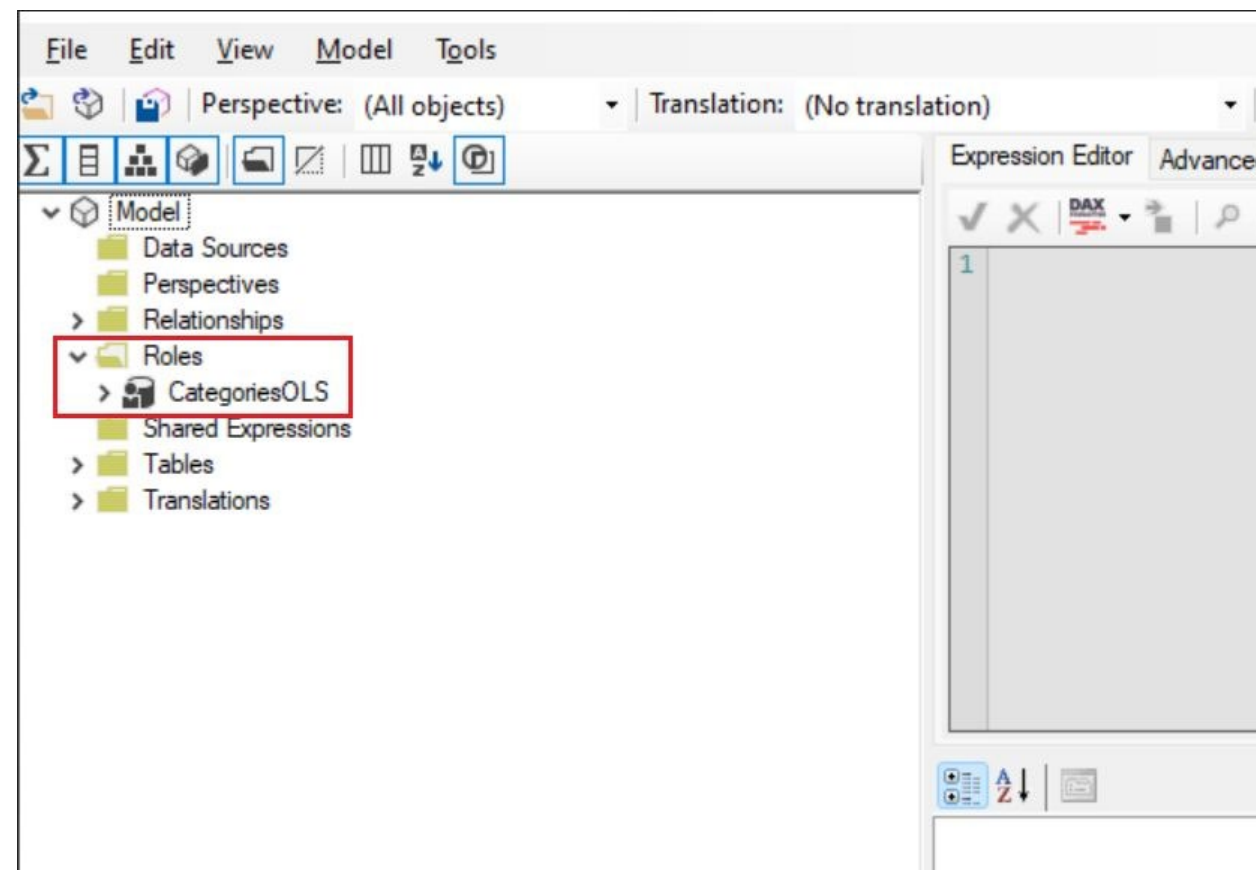
- Set up RLS by creating one or more roles.
- You can create, validate, and manage roles in Power BI Desktop.
- Manage roles
 - For Azure Analysis Services or SQL Server Analysis Services models, you can create, validate, and manage roles by using SQL Server Data Tools (SSDT).
 - Can also create and manage roles by using SQL Server Management Studio (SSMS), or by using a third-party tool, like Tabular Editor.

Row-level Security

- In the Power BI service, you can add a member to the role by typing in the **email address** or name of the user or **security group**.
- You can't add Groups *created in Power BI*.
- You can add members external to your organization.
- You can use the following groups to set up row level security.
 - Distribution Group
 - Mail-enabled Group
 - Microsoft Entra Security Group

Object-level security (OLS)

- **Object-level security (OLS)** enables model authors to secure specific **tables** or **columns** from report viewers.
- OLS only applies to **Viewers** in a workspace.
- OLS is defined within model roles. Currently, you can't create OLS definitions natively in Power BI Desktop.





Semantic Model Access



Semantic Model Access

- **Share data** of your **semantic model** with other users.
- Grant User Permissions:
 - Read
 - Build
 - Reshare
 - Write

Users with **Build** Permissions can perform the following actions:

- Export underlying Power BI data.
- Build new content on the semantic model

Share dataset
 Sales Operations

AV Adele Vance

Enter a name or email address

☒ Allow recipients to modify this dataset

☒ Allow recipients to share this dataset

☒ Allow recipients to build content with the data associated with this dataset

☒ Send an email notification

Add a message (optional)

Grant access

Cancel

Semantic Model Permissions

Permission	Description
Read	<p>Allows user to access reports and other solutions, such as composite models on Premium/PPU workspaces, that read data from the semantic model.</p> <p>Allows user to view semantic model settings.</p>
Build	<p>Allows user to build new content from the semantic model and find content that uses the semantic model.</p> <p>Allows user to access reports that access composite models on Power BI Pro workspaces.</p> <p>Allows user to build composite models.</p> <p>Allows user to pull the data into Analyze in Excel.</p> <p>Allows querying using external APIs such as XMLA.</p> <p>Allows user to see hidden data fields.</p>
Reshare	<p>Allows user to grant semantic model access.</p>
Write	<p>Allows user to republish the semantic model.</p> <p>Allows user to backup and restore the semantic model.</p> <p>Allows user to make changes to the semantic model via XMLA.</p> <p>Allows user to edit semantic model settings, except data refresh, credentials, and automatic aggregations.</p>
Owner	<p>The semantic model owner isn't a permission in itself, but rather a conceptual role that has all the permissions on a semantic model. The first semantic model owner is the person who created the semantic model, and afterwards the last person to configure the semantic model after taking it over in the semantic model settings.</p> <p>In addition to the permissions described in this table that can be granted explicitly, a semantic model owner can configure semantic model refresh, credentials, and automatic aggregations.</p>

Permissions by workspace role

A user's role in a workspace implicitly grants them permissions on the semantic models in the workspace, as described in the following table.

	Admin	Member	Contributor	Viewer
Read	✓	✓	✓	✓
Build	✓	✓	✓	✗
Reshare	✓	✓	✗	✗
Write	✓	✓	✓	✗



Sensitivity label



Sensitivity Label

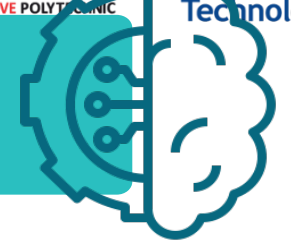
- Classify critical content in Power BI without compromising productivity or the ability to collaborate.
- In the Power BI service, sensitivity labels can be applied to
 - semantic models,
 - reports,
 - dashboards,
 - dataflows.
- In Power BI Desktop sensitivity labels can be applied to .pbix files
 - Example: only users within your organization can open a confidential .pbix that has been shared or attached in an email),

Sensitivity label

Sensitivity

- Non-business
- Public
- General
- Confidential
- Highly Confidential

Knowledge Check



Share Dashboard & Report

1. If colleagues need to keep the report up to date, or need access to all the content in the workspace.
2. If colleagues just need to view the content in the workspace.
3. If colleagues just need to see that report and not all the content in the workspace.
4. If the report is better consumed with related reports or dashboards that you need to distribute to many colleagues.

Add to workspace as **Viewer**

Publish an **app**

Add to workspace as **Member**
or **Contributor**

Share the report via link

