Securing datasets in Power BI Service

DEPLOYING AND MAINTAINING ASSETS IN POWER BI

Kevin Feasel
CTO, Faregame Inc

datacamp

Dataset permissions

Read

- Allow users to access reports which read data from the dataset
- Does NOT allow users to find content which uses a dataset
- Does NOT support external API queries

Reshare

- Allow users to share dataset contents with other users
- Can grant Read, Reshare, or Build permissions to other users

Build

- Allow users to build new content from a dataset
- Allow users to find content which uses a dataset
- Allow users to query using external APIs

Write

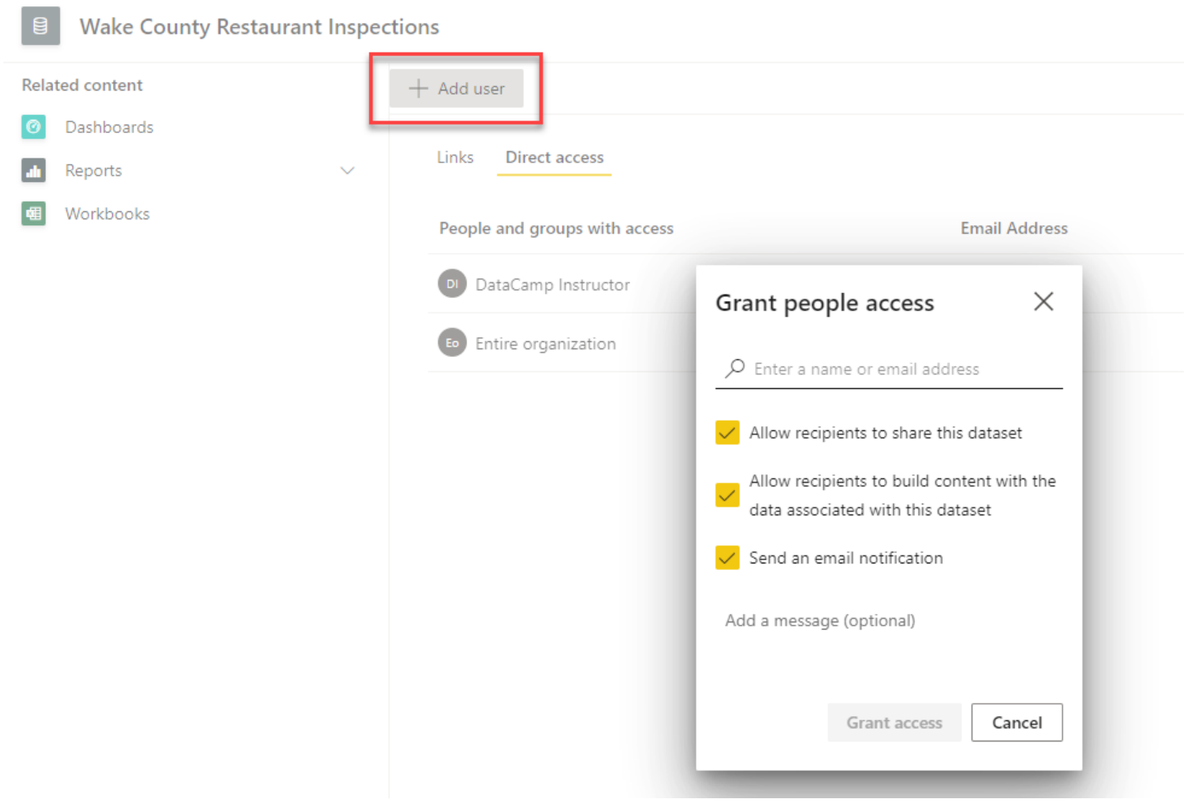
- Allow users to view and modify dataset metadata

Datasets and workspace roles

	Admin	Member	Contributor	Viewer
Read	Yes	Yes	Yes	Yes
Build	Yes	Yes	Yes	No
Write	Yes	Yes	Yes	No
Reshare	Yes	Yes	No	No

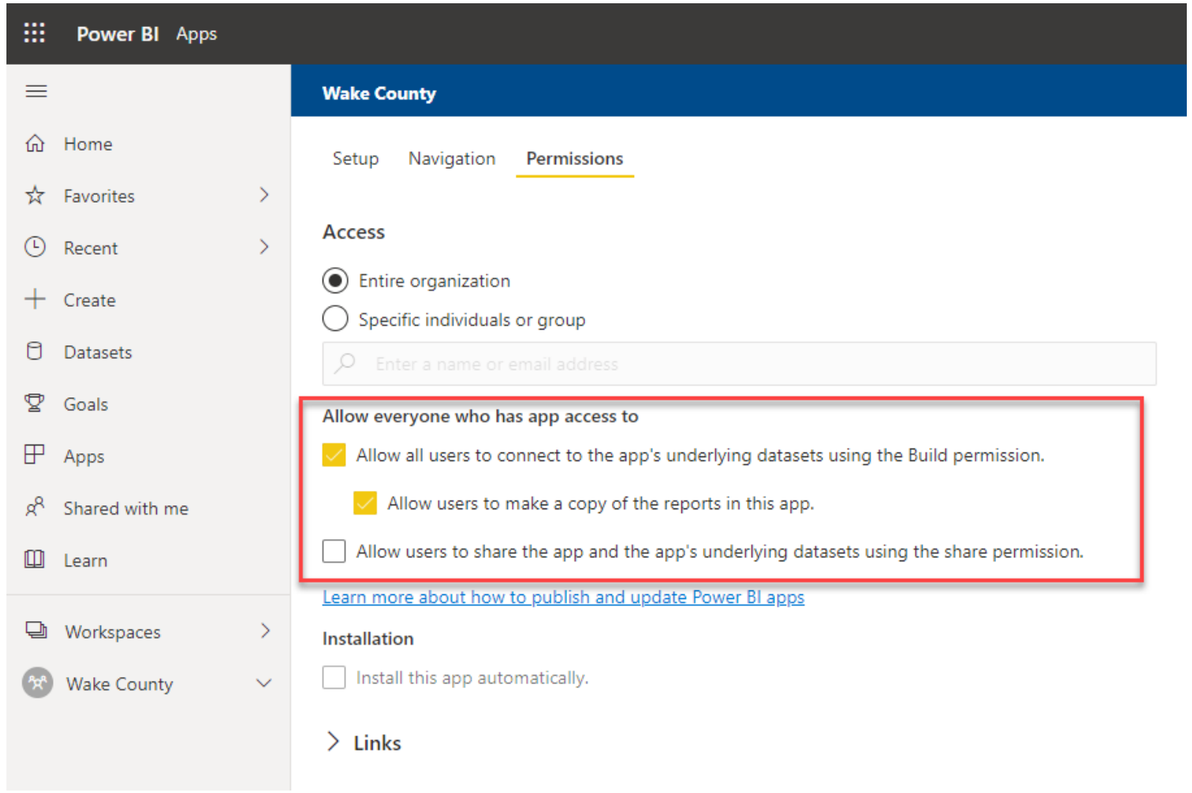
Ways to obtain dataset permissions

- Directly grant dataset permissions to a user or group



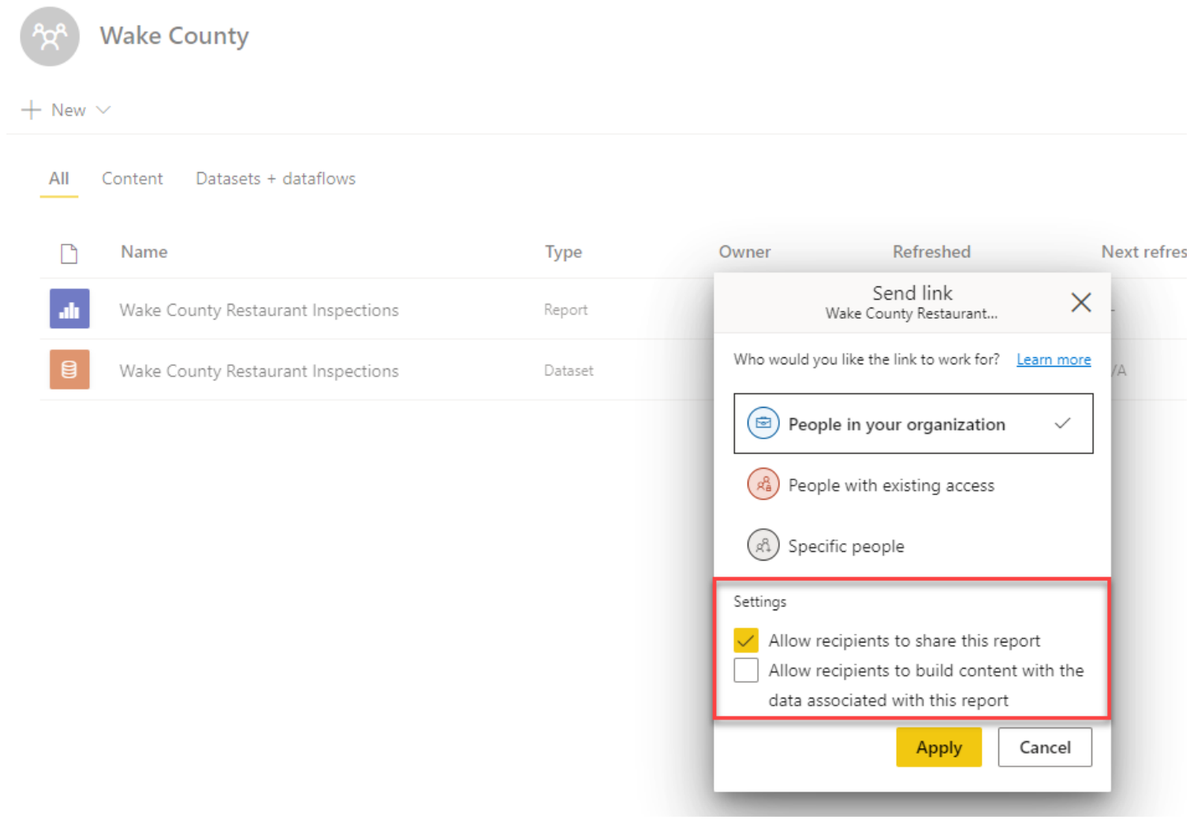
Ways to obtain dataset permissions

- Directly grant dataset permissions to a user or group
- Grant permissions to an app and let the user get the app



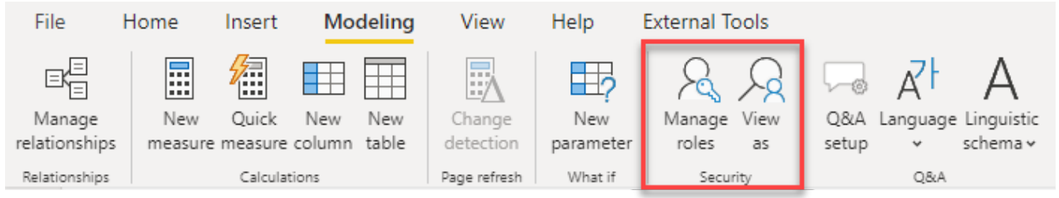
Ways to obtain dataset permissions

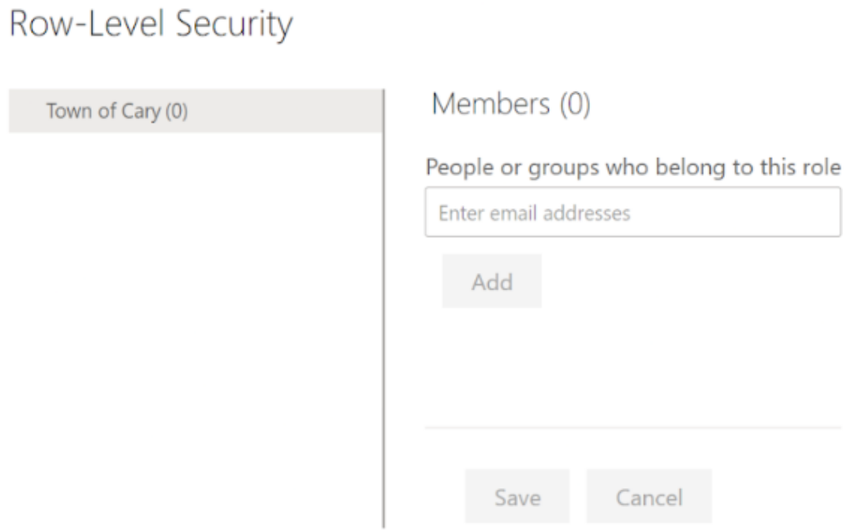
- Directly grant dataset permissions to a user or group
- Grant permissions to an app and let the user get the app
- Share a link to a report



Row-level security (RLS)

- Restrict data access for given users
- Create filters to show or hide specific rows based on the current user's access rights
- Filters defined for **roles**
- Use Power BI Desktop to define roles
- Use Power BI Service to assign users and groups to roles



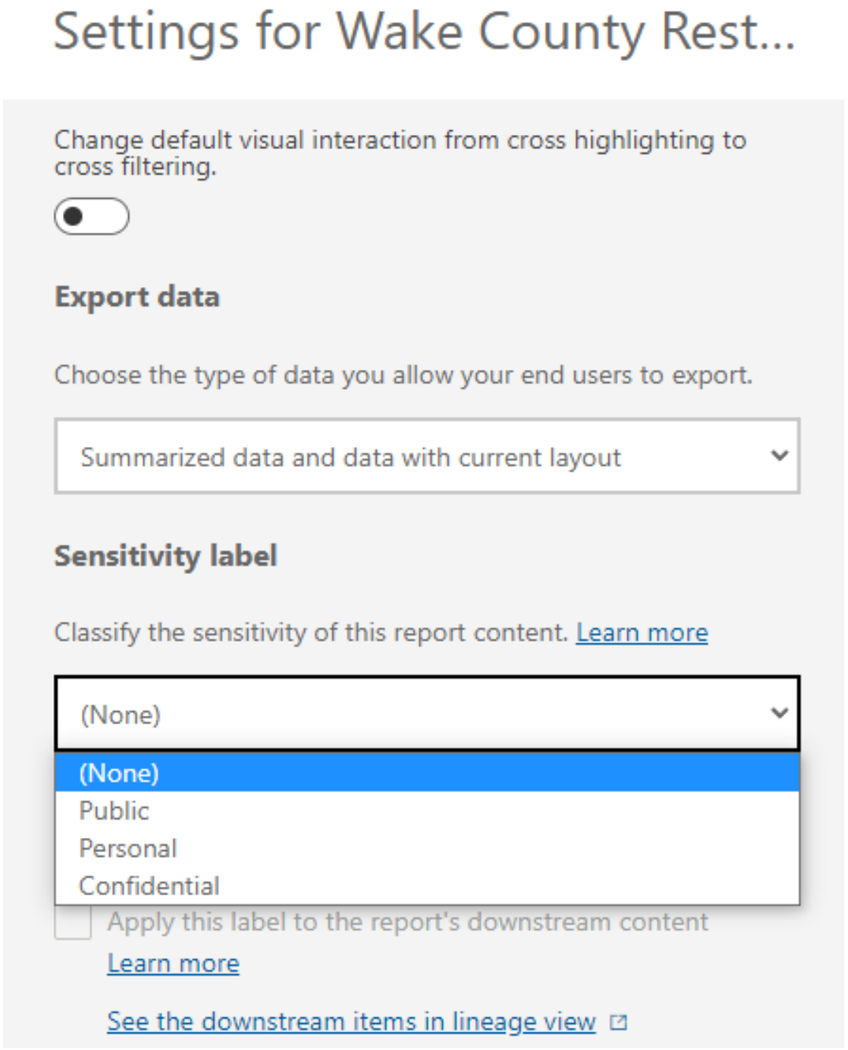


Row-level security limitations

- Performance will be slower due to additional processing requirements
- Users with dataset Write permissions will see all data--in practice, row-level security is limited to Viewers

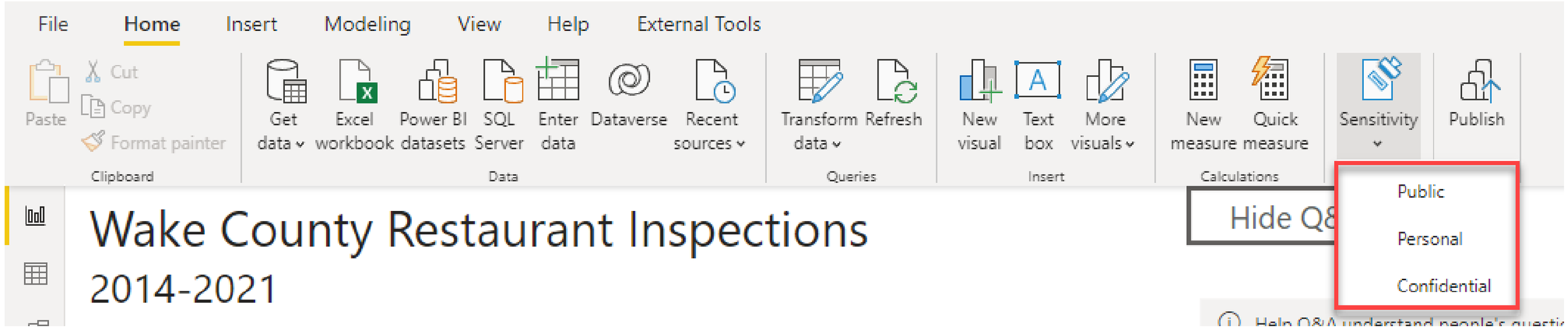
Sensitivity labels

- Guard sensitive content against unauthorized data access and leakage
- Sensitivity labels with encryption settings may affect access to content in Power BI Desktop
- Power BI admins can block export of sensitive data
- Sensitivity labels may change--people with the ability to set sensitivity labels may change them
- All changes are tracked in the Power BI audit log



To set sensitivity labels

- Sensitivity labels must be set up in the Microsoft 365 Compliance Center
- Sensitivity labeling must be enabled for the organization
- Must be logged in
- Must have Power BI Pro or Premium Per User license
- Must have edit permissions on the content you wish to label



Let's practice!

DEPLOYING AND MAINTAINING ASSETS IN POWER BI

Manage dataset permissions

DEPLOYING AND MAINTAINING ASSETS IN POWER BI

Full Name
Instructor

datacamp

Let's practice!

DEPLOYING AND MAINTAINING ASSETS IN POWER BI

Apply sensitivity labels

DEPLOYING AND MAINTAINING ASSETS IN POWER BI

Full Name
Instructor

datacamp

Let's practice!

DEPLOYING AND MAINTAINING ASSETS IN POWER BI