Project Management Insights - Power BI

Introduction

The BrightWork 365 Project Management Insights - Power BI report gives insights into who is accessing BrightWork 365; what audited changes are being made to records; what areas are being interacted with; and who is making the most changes. This information can be used to improve and evolve your organization's Project and Portfolio Management practices.

> **Note**
> - The report only works if you have auditing enabled in your organization and can only report on the number of days that you have set to retain audit logs for. You can see this setting on your environment's home page in https://admin.powerplatform.microsoft.com.
> - The Project Management Insights report is designed to be used only by a BrightWork PMO Manager security role holder.

> **Tip** See also Power BI Dashboards Overview which includes general usage information.

Accessing the Report

1. Click **Reporting** in the Portfolios section of the main navigation.
2. In the Dashboards drop-down, select **11. Project Management Insights - Power BI**.
3. Select one of the available report pages at the bottom of the screen.

Report Pages

There are 5 pages in the report:

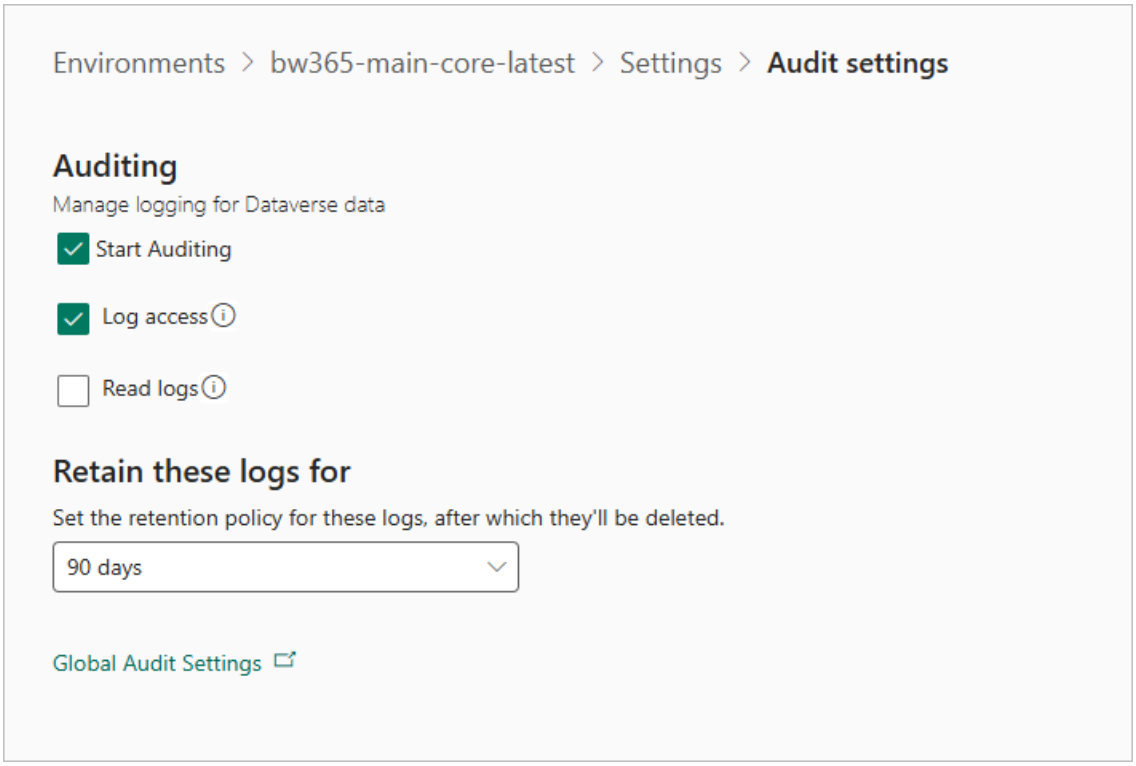
- User Access
- Audit History
- RTF Audit History
- Project Management Interactions
- User Interactions

User Access

The User Access page shows which users have accessed BrightWork 365 and which day they accessed the environment in which BrightWork 365 is installed.

This User Access report can generate false positive access records if a user has a process running under their identity. For example, the Conor Dever user below does not have a BrightWork 365 license but shows up in the report as they are the owner of a number of tenant-level process running under the Center of Excellence environment.

The user access report requires Log access to be enabled in the Environment's Audit settings. Also note the retention policy setting in the screenshot. When setting up the report, users will decide on the number of days into the past that the report will display. The available days depend on the environment's retention policy setting - the report can only report on what is available.



Audit History

The Audit History page provides a detailed cross-record and cross-table view into all recent audited changes.

This page includes slicers on Project, Table, Columns, User and Date. This means for example that you can use the Project slicer to see all changes made to all records in a project in a single view.

Rich Text Audit History

This page includes a means for viewing edits made to RTF columns. RTF columns are stored as HTML in the database. This can make the changes difficult to understand when viewed as an audit record. This report uses a HTML viewer to render the change on a column-by-column basis.

Although images are not viewable and will appear as broken links in the report page, you will be able to view associated actions. e.g., an image was added or was removed.

Click on a column in the report to see the before and after changes for the column in question.

Project Management Interactions

This page shows a summary of the different interactions on a table-by-table basis. The types of interaction include Create and Update for most tables and Access for the User table.

User Interactions

This page is similar to the Table Interactions page, but it includes a user dimension. This is probably the best way to assess user activity. The total interaction count for a user is a combination of their specific record interactions plus their general access to records.

Report Security

> **Note** See also Portfolio Security & Access.

The Project Management Insights report includes optional row level security (RLS) and uses business units as the filter. The means that when a user, with Viewer access to the workspace in which the report is published logs in and views the report, they should only see information about the users and records that their Business Unit allows them to see.

Every row in the audit table relates to another row in Dataverse. The report applies the Owning Business Unit of the related row to the row in the audit table and uses it and the logged-in user context (i.e., their Business Unit) to filter the data displayed to the logged-in user.

When RLS is enabled in the report, the following occurs:

- Logged-in Viewer users only see the items that their Business Unit allows them to see. They will not see items in confidential projects to which they have access by virtue of being added as a team member with Edit access.
- Information regarding Deletes are excluded from the report. This is because as a deleted record no longer exists, we are unable to get its Owning Business Unit to apply the security filter. This

could result in sensitive information being made available to the logged-in user.
- Only nominated tables are included in the report. See Adding Custom Tables to the Report below.

If you want to further restrict access to the report, do not publish it to a general workspace. Either use a workspace that only the allowed users have access to or create a specific workplace for the report and add the desired users as viewers to the workspace.

Once you publish the report, you will have to add each report user to the RLS security group associated with the report's semantic model. You can also add an Entra Security group instead of adding users one by one. See https://devoworx.net/using-groups-to-manage-rls-roles-in-power-bi/ for a third-party article that discusses this topic. Users with Viewer access to the Power BI workspace will not be able to access the report until you do this.

> **Caution**
> - Make sure to not make yourself a Viewer in the workspace - doing so means you will lose your admin access to the workspace.
> - Users with greater than Viewer access to the Power BI workspace will be able to view the report without being added to the RLS security group. The RLS filter only works on users with Viewer access.
> - If a user is moved to a new business unit, this will not be reflected until the next time the report is refreshed in the service. You can do a manual refresh if you want the change to be reflected sooner.

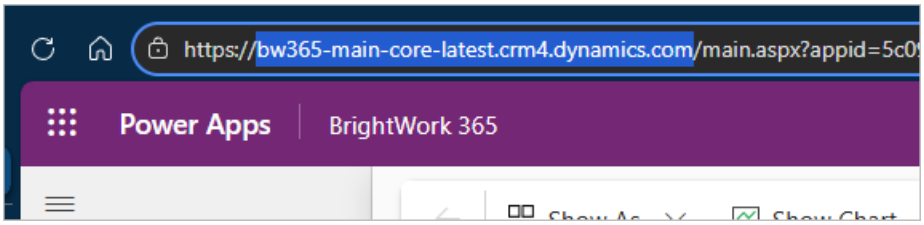
See https://learn.microsoft.com/en-us/power-bi/guidance/rls-guidance for more information about RLS and https://learn.microsoft.com/en-us/power-bi/collaborate-share/service-roles-new-workspaces for more information about roles in Power BI workspaces.

Lastly, you do not have to publish the report to the Power BI service - you can just use it in desktop mode if you desire.

Report Setup Steps

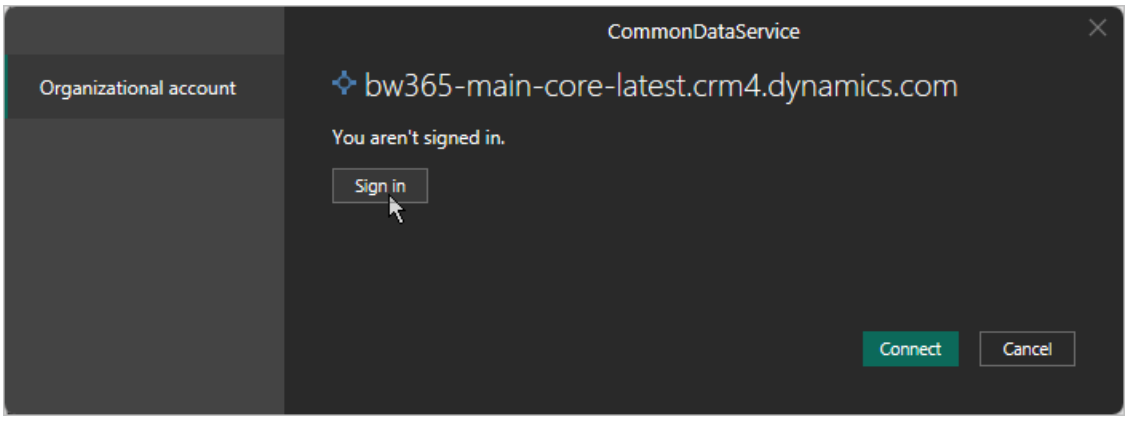
For this section you will need the Power BI Desktop app. You can download it from the Microsoft Windows app store. You will also need at minimum a Power BI Pro License to publish the report to a shared workspace.

1. Copy the URL of the environment into which BrightWork 365 is installed without the https:// bit - as shown below.



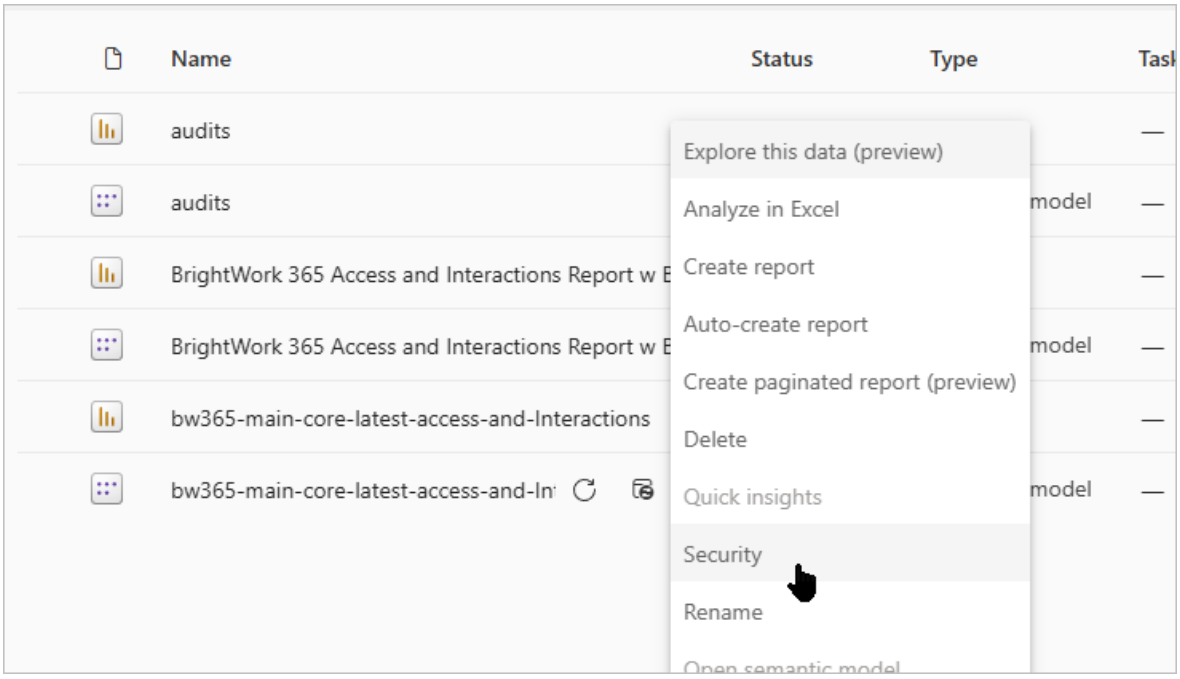
2. Double-click on the BrightWork 365 Access and Interactions Report.pbit file to open it in Power BI desktop - a window will open requiring you to enter content.
3. Enter TRUE for the Enforce RLS field if you want to use RLS to apply business unit report security or FALSE if you do not (see the Report Security section above).
4. Enter the number of days to query - we recommend starting with 90.
5. Paste in the copied URL and click **Load**.

6. Click **Sign in** and then click **Connect** - this will happen twice.

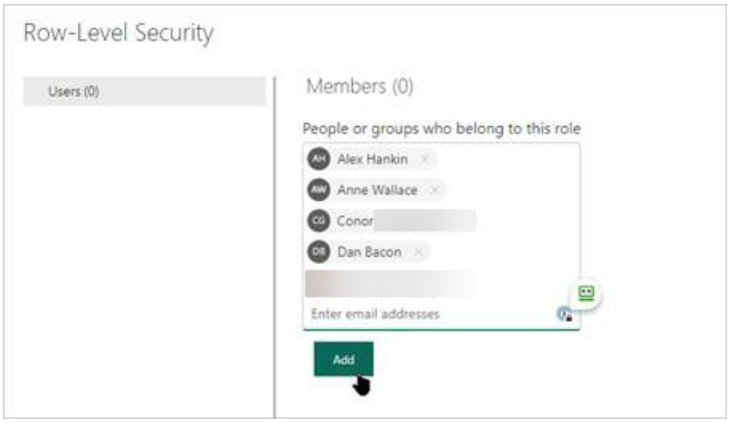


7. Save the report to your desktop and publish it to a workspace of your choice (see the Report Security section above).

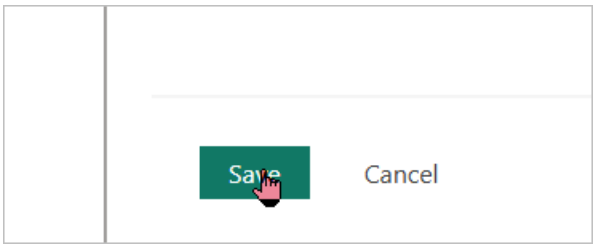
8. Navigate to the workspace and click **Security** on the three-dot menu associated with the semantic model.



9. Start typing the name of the user or Entra group you want to add or paste in email addresses and click **Add** (you can paste the email address in one go).



10. Click **Save**.



11. Ensure that the users that you want RLS to be applied to have Viewer level access to the workspace.

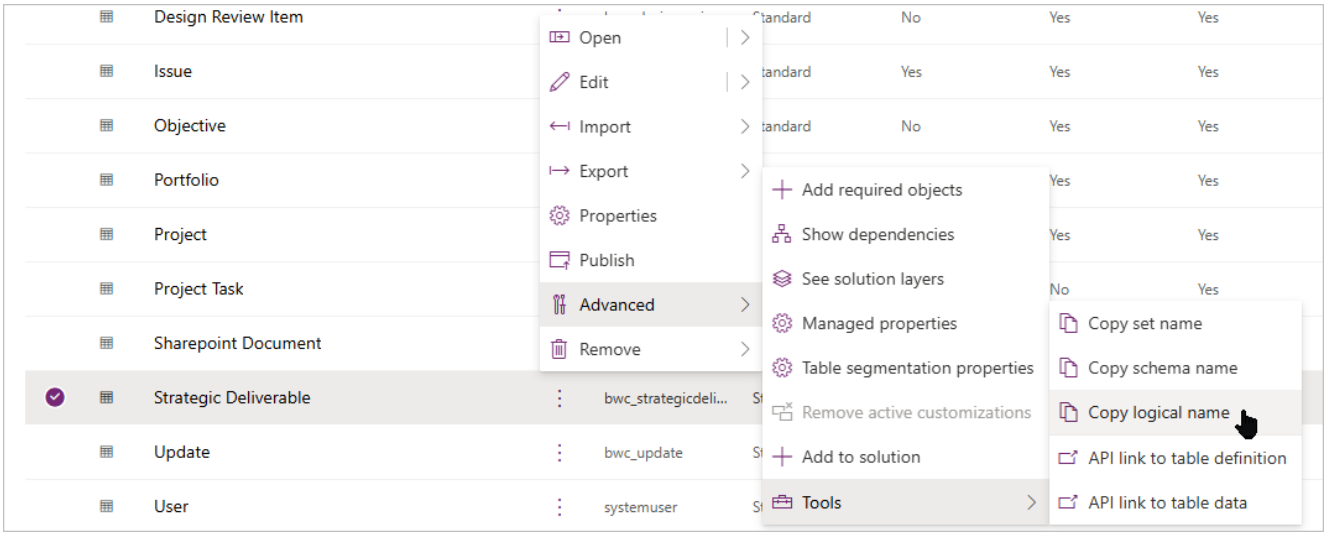
Caution

- You still need to add all Viewer users to this role even if you set Enforce RLS to false.
- Make sure to not make yourself a Viewer in the workspace - doing so means you will lose your admin access to the workspace!

Adding Custom Tables to the Report

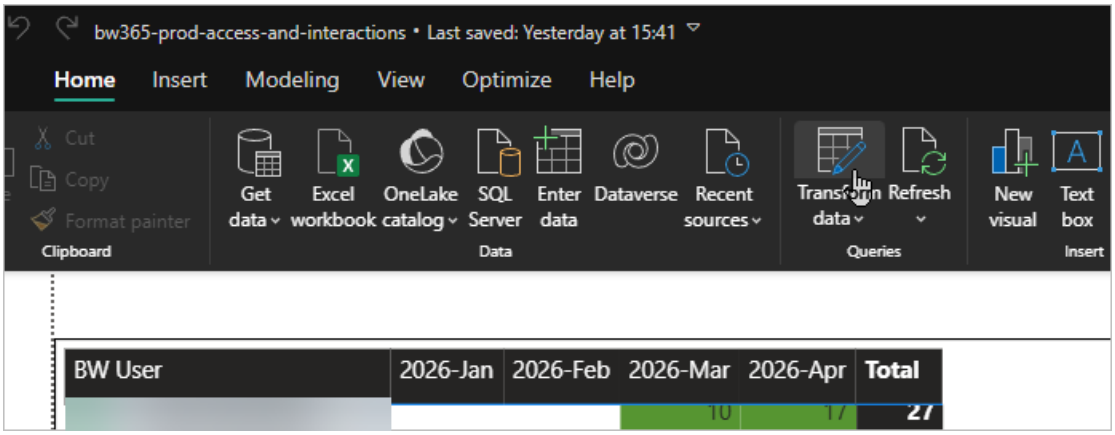
The out of the box Project Management Insights - Power BI report only reports on the default BrightWork 365 tables; however, if you are comfortable with working with Power BI desktop, you can edit the report to include your local custom tables.

To update the report, you will first need to gather the logical names of the tables that you want to add to the report. You can get this from the make area of your custom solution or from the URL when viewing a table in the BrightWork 365 app.

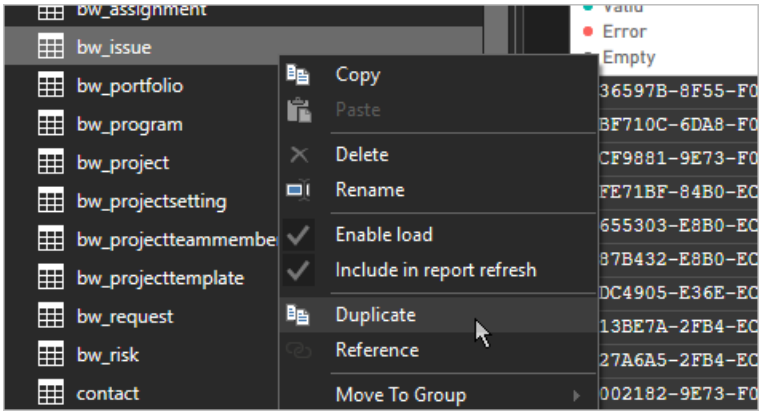


To add custom tables to the report:

1. Open the report in Power BI desktop and click **Transform Data** to open the Query Editor for the report.

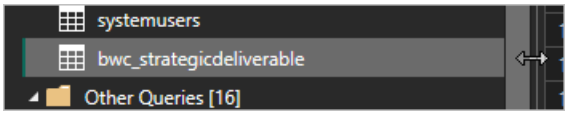


2. Right click on **bw_issue** and click **Duplicate**.

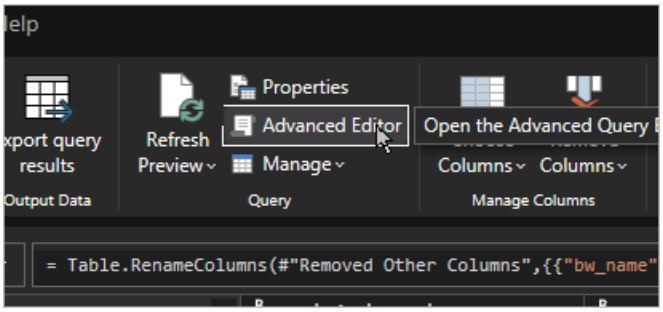


3. Double click on the copied table and rename it to the logical name of the table that

you want to add.

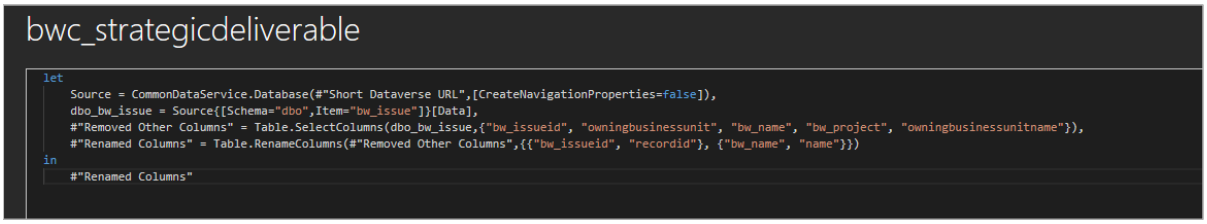


4. With the copied table still selected, click on **Advanced Editor**.

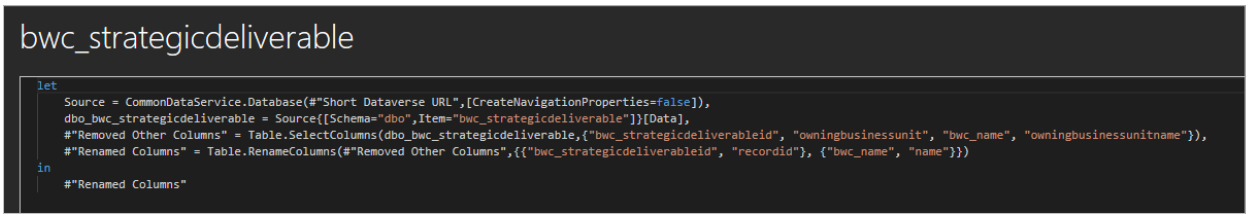


5. Update the code as follows and see below for the Before and After image.
    a. Replace bw_issue with the logical name of your table.
    b. Update bw_name to what it is in your table (likely bwc_name).
    c. If your table does not have a relationship with the Project table in BrightWork 365, remove "bw_project", from the code (our example includes this change).

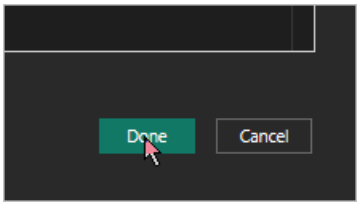
Before



After

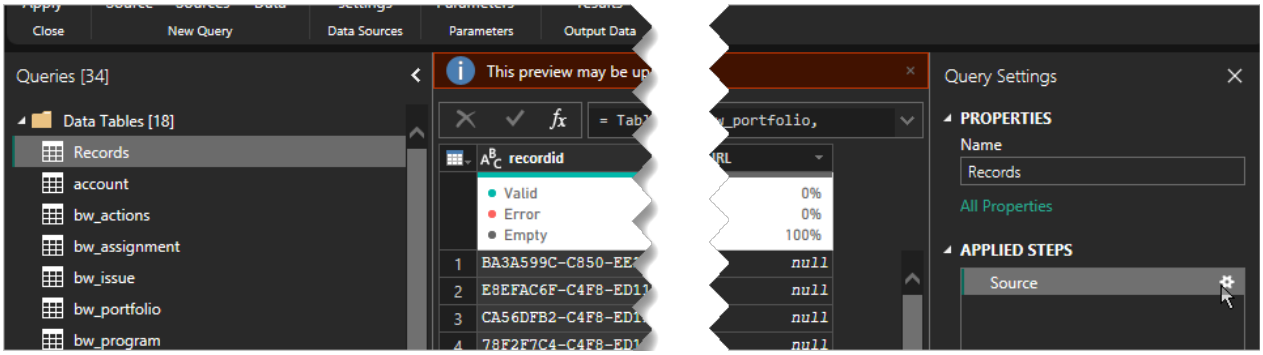


6. Click Done.

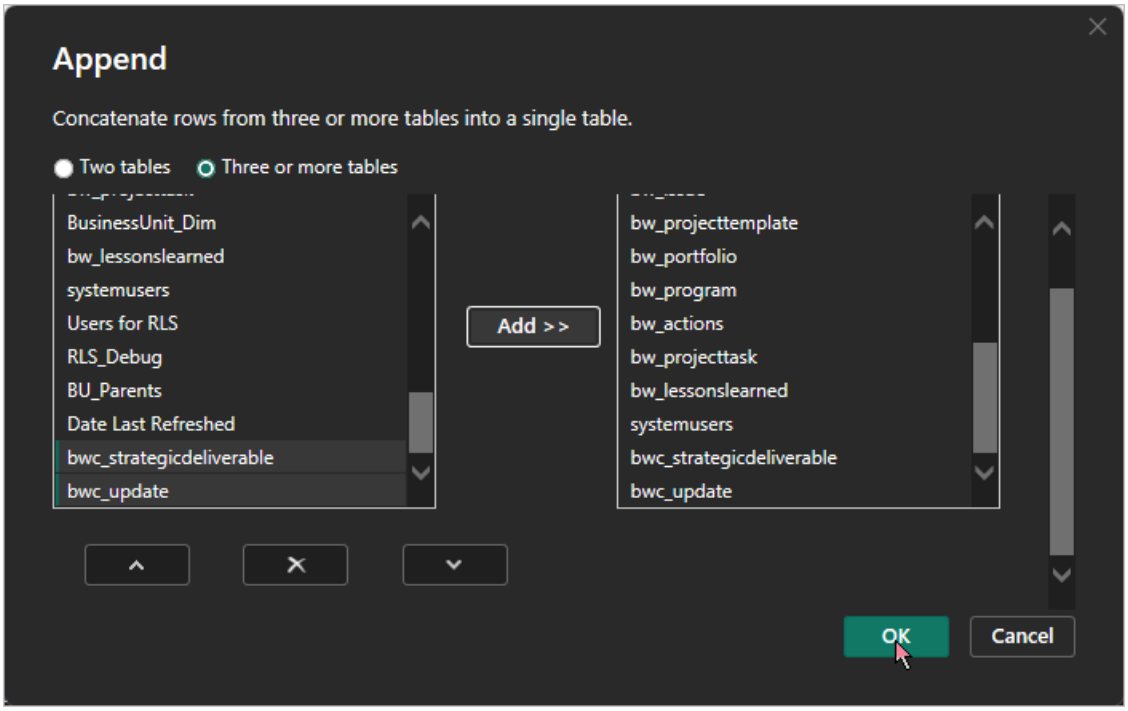


If you get an error, review your changes according to the error.

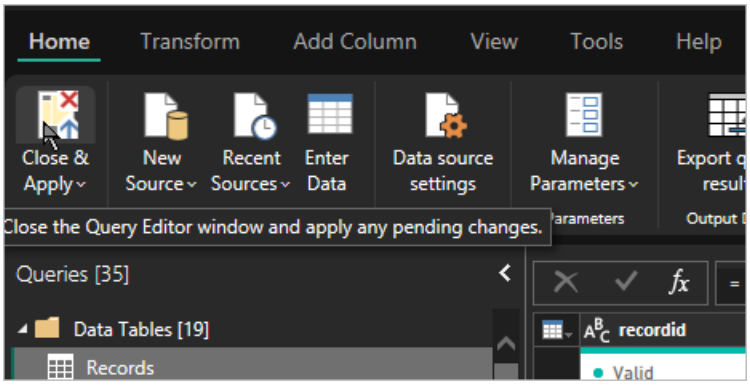
7. Repeat the above steps for any other custom tables you want to add.
8. Click **Records** in the same group and click edit Source in the Query Settings area.



9. Select your custom tables, click **Add** and click **OK**.



10. Click **Close and Apply**.



The report will now refresh in Power BI Desktop, and you can republish it when you are ready.