Security and Power BI Reports

BrightWork 365 supports the option to implement business unit security in Power BI reports, with some caveats noted below. Business unit security is enabled by setting the enforcement of Row Level Security (see Microsoft Learn article) to True in the Power BI report (see the Implementing Business Unit Security section below).

BrightWork 365 ships with 4 Power BI reports:

- My Work
- Resource Utilization
- Portfolio and Projects
- Project Management Insights

> **Note**
> - The legacy Documents report, which no longer ships with BrightWork 365, is not in scope for security restrictions. If you are implementing security, you should hide this report as it may allow users to become aware of the existence of confidential projects.
> - Changes that will impact the report, for example moving a user to a different Home Business Unit, will only be reflected in the report after it has refreshed.

> **Caution** Users with greater than Viewer access to Power BI report workspaces are not affected by report security and can therefore access confidential reports.

My Work

The My Work Power BI report uses Row Level Security to only show the logged in user their assigned work. If a user is assigned work in a confidential project to which they do not yet have access, they will unfortunately see those work items in this report.

If this is an issue, then you should not publish this report. User can use the My Work link on the BrightWork 365 left navigation. This view will not show them items to which they do not yet have access.

Resource Utilization

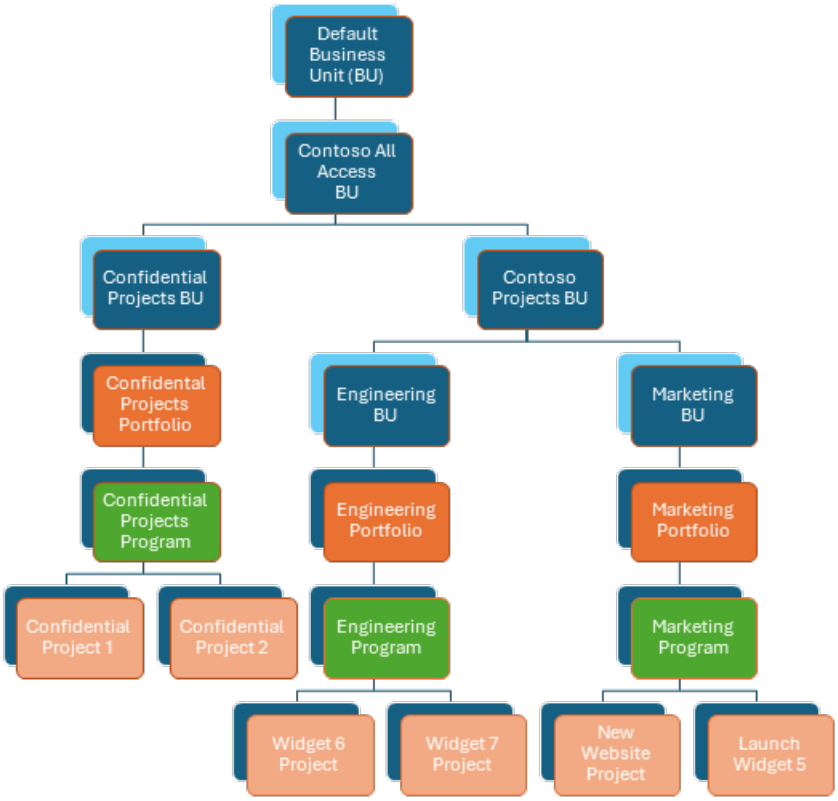
The Resource Utilization is designed to enable project managers assess the availability of users in the organization for work. As such, it should be a global report.

If you are implementing security, you should hide the Resource Dashboard page in the Resource Utilization report before publishing, as it may allow users to become aware of the existence of confidential projects.

Portfolio and Projects

The Portfolio and Projects report uses a user's home business unit and below to only display items in that context. This means that users given access to confidential projects outside of their business unit context will not see these projects in the report.

A further limitation of the home business unit-only approach lies with users given the BrightWork PMO Manager security role. In the BrightWork 365 app, this role gives these users access to all items, regardless of their home business unit. This will not happen with the Portfolio and Projects report if these users are in a lower level business unit. The remedy here is to put users with the BrightWork PMO Manager security role in the top business unit – in the image below this would be the Default Business Unit.



Project Management Insights

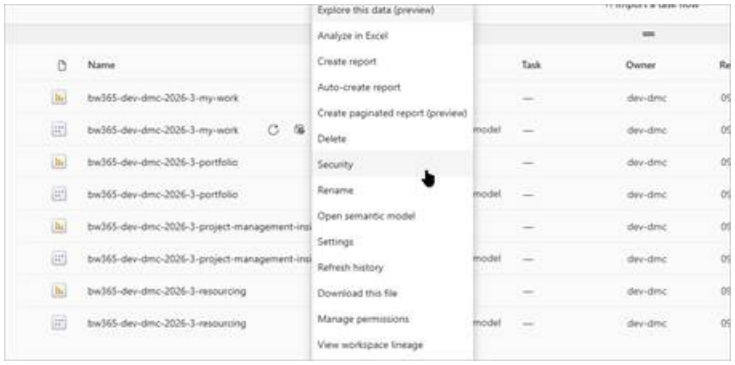
The Project Management Insights report is designed as a BrightWork PMO Manager only report.

As with the Portfolio and Projects report noted above, you should ensure that all users with the BrightWork PMO Manager security role are in the Default Business Unit to ensure proper report access.

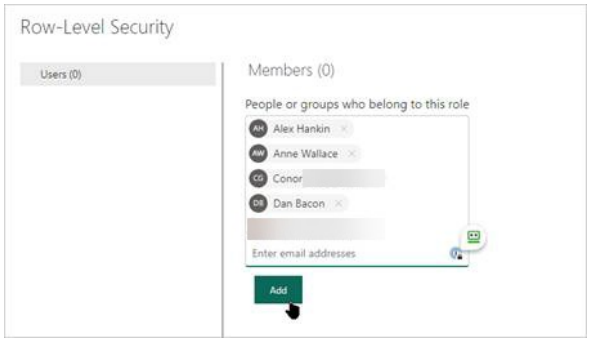
Giving Users Report Access

BrightWork 365 reports utilize Row Level Security (RLS) to filter Power BI reports for the user context. RLS only works for users added to the report workspace as Viewers. It will also only work for these Viewer users when they are also added to the RLS security profile associated with the report (users with greater than Viewer access will be able to view reports without being added to the RLS security group). This step must be carried out even if RLS is set to False in the report.

1. Login to https://app.powerbi.com/ and navigate to the workspace into which you published the reports.
2. Click **Security** on a report dataset menu.



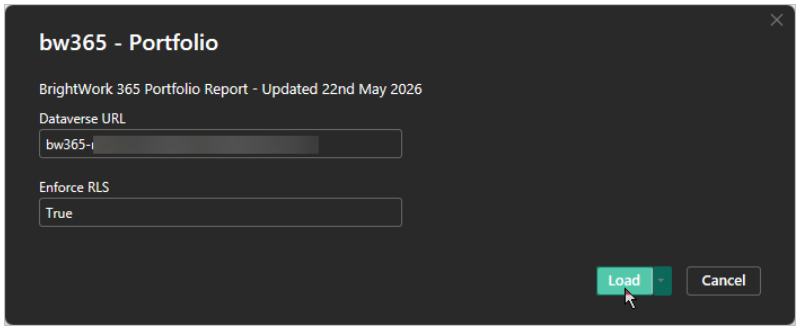
3. Add each user who will be accessing the report, click **Add**, and click **Save** when done. You can also add a team in which the users are a member.



Implementing Business Unit Report Security

Business Unit report security can be implemented for the Power BI reports that support it (see the Security and Power BI Reports section above), by choosing to Enforce Row Level Security (RLS) when setting up the Power BI PBIT.

Enforce RLS = True means business unit report security is enabled. Enforce RLS = False means business unit report security is not enabled:



This option is also available in the Power BI service on the report settings page:

