Portfolio Security & Access

> Video has been removed from this PDF. Visit the BrightWork 365 knowledge base to view.

Project Management Context

Organizations do not always want to have entirely open access to their portfolio of projects but rather need to take a more granular approach to security and access, while others are fine with users having access to the entire portfolio of projects. BrightWork 365 provides several options to accommodate both of these security requirements through a flexible security and access model that includes business units, portfolios, and projects.

See also Project Security & Access.

Your browser does not support HTML5 video.

What's In Scope and Out of Scope for Security & Access?

Items Included in Security & Access	Items Excluded from Security & Access
• Portfolios • Programs • Projects • Team Member Security • Default Team Member Access • Status Reports • Risks • Issues • Actions • Costs • Custom table support (via customizations)	• SharePoint • Power BI with some exceptions (see the Security and Power BI Reports section below) • Microsoft Teams • Requests • Content Templates ◦ By default, Content Templates are part of the top-level Default business unit. Users who are only given security roles at lower business unit levels will not be able to create projects from Project Templates associated with these Content Templates. Contact your Customer Success Partner for configuration methods to work with this scenario.

Caution

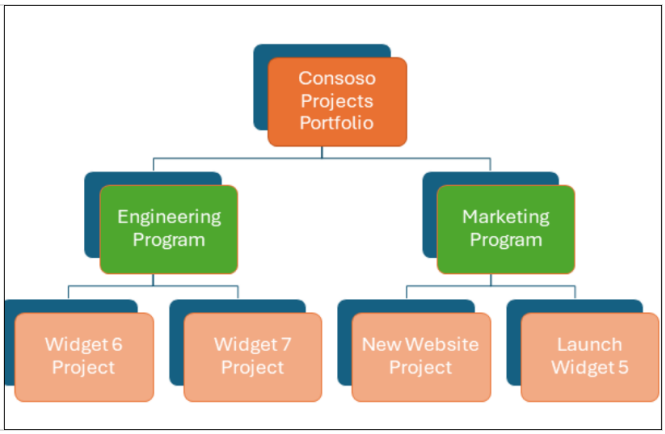
- Due to the items excluded from Security & Access noted in the table above:
  - If you have confidential programs and portfolios, do not create templates with

confidential information, and leave the Portfolio and Program fields blank, otherwise everyone can potentially become aware of their existence.
    - Customers are advised to use generic names for confidential projects as the project names will be visible to all users in these and other various places in the app.
    - Remove from the Power BI workspace those users that you do not want to view confidential projects, since these projects will be displayed in Power BI dashboards.
- Users with the BrightWork PMO Manager security role have access to everything in BrightWork 365, including confidential projects, regardless of the chosen security model or their assigned business unit.
- Security will not work if you have customized any out of the box BrightWork 365 security roles. If necessary, create your own custom security roles instead. If you have already customized any of the BrightWork 365 security roles in a custom solution, security is not going to work until you upgrade the environment that the unmanaged version of the custom solution is in and reimport the managed custom solution into the environment.
- If you have an unmanaged layer on any of the out of the box BrightWork 365 security roles, security is not going to work until you remove it.

Security Model 1: Open Access (default model)

In the default open access model, all BrightWork 365 users have access to all portfolios, programs, and projects within the BrightWork 365 app. Note that this open access can be mixed together with a restricted security model as needed.

Example: Single Open Portfolio



- One business unit and one portfolio with access to all app content.
- All users have access to all portfolios, programs, and projects.

Security Model 2: Portfolio Security

The Portfolio Security model explained in this article uses Power Platform business unit membership (see Microsoft article) combined with BrightWork security roles to grant users

access to a portfolio attached to a business unit, and all the portfolio's child projects and records.

The BrightWork 365 business unit setup for Security and Access can divide access into a Confidential Projects and a Contoso Projects hierarchy ("Contoso" is being used as a sample organization name). Further business units can then be created to minimize access and more easily manage restrictions, as required.

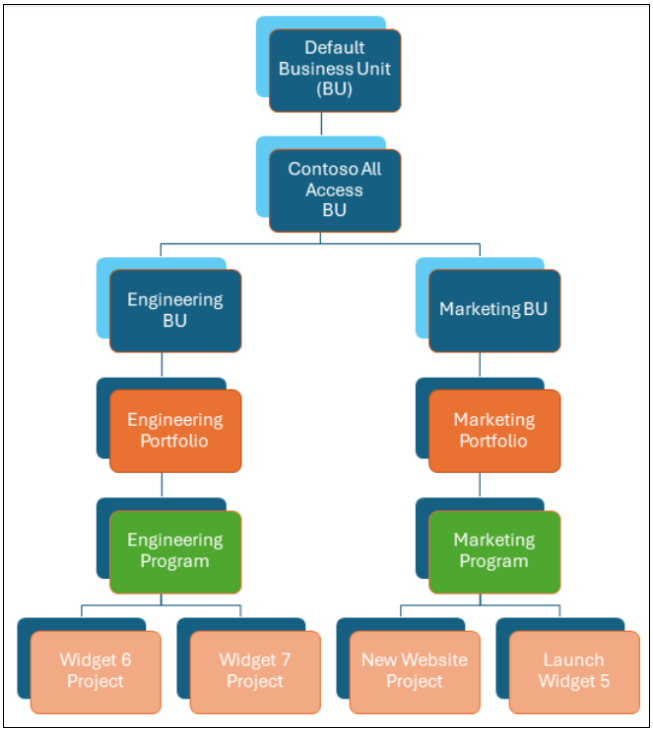
The high-level steps to implement are as follows (further details in other article sections below):

1. Create business units and a business unit hierarchy.
2. Assign BrightWork 365 users to a home business unit.
3. Assign users security roles in their home business unit.
4. (Optional) Assign users the same security role they have in their home business unit in secondary business units as needed.
5. Create portfolios that will act as the top parent levels of the hierarchy in BrightWork 365.
6. Within each portfolio select an Owning Business Unit.
7. Assign programs to a portfolio associated with the business unit desired for the program and its child projects.

After the above steps are completed, users will have access to the portfolios, programs, and projects that are associated with the business units in which they have been given security roles.

> **Tip** In the My Work > All Work view, users will only ever see the users and assignments for people in their Business Unit.

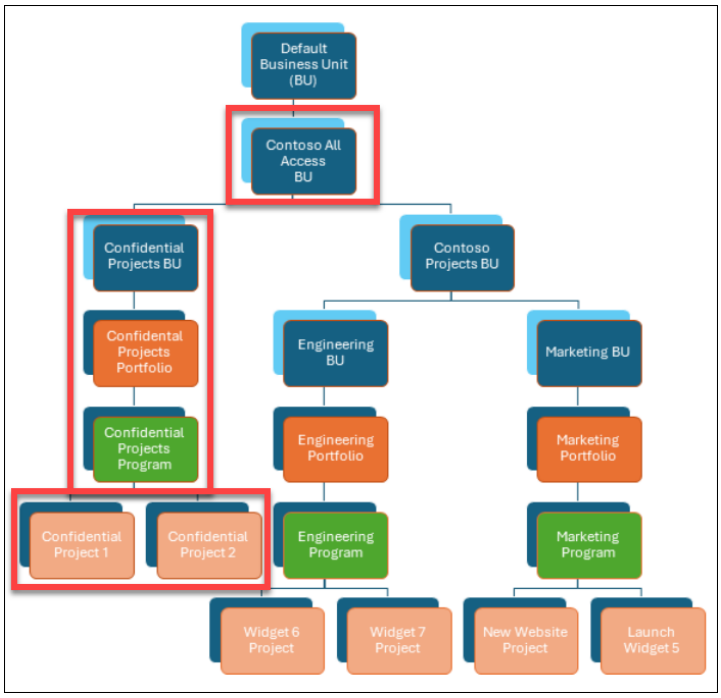
Example: Projects Secured by Department



- Engineering users are added to the Engineering business unit and only see its portfolio, program, and projects.
- Marketing users are added to the Marketing business unit and only see its portfolio, program, and projects.

> **Tip** A user can be given the same security roles in both the Engineering and Marketing business units so that they have access to both sets of portfolios, programs, and projects.

Example: Portfolio Security with Confidential Projects

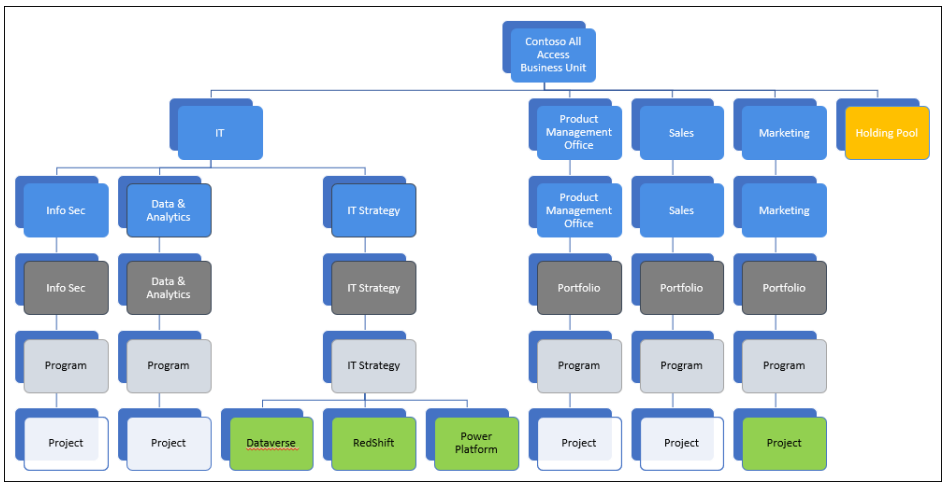


- Users who need access to all confidential and non-confidential projects would be in the parent Contoso All Access business unit.
- Users who need to see only non-confidential projects would be in the Contoso Projects business unit.
- If users should only be given access to individual confidential projects by exception instead of all projects in the Confidential Projects portfolio, then instead of giving them access via membership in the Confidential Projects business unit, you would give them access to the individual projects from within each project using Project Security and Access.
    - This exception project access is managed by the Access Level in each project team member record in each individual confidential project.

Security Model 3: Portfolio Security with Project Security

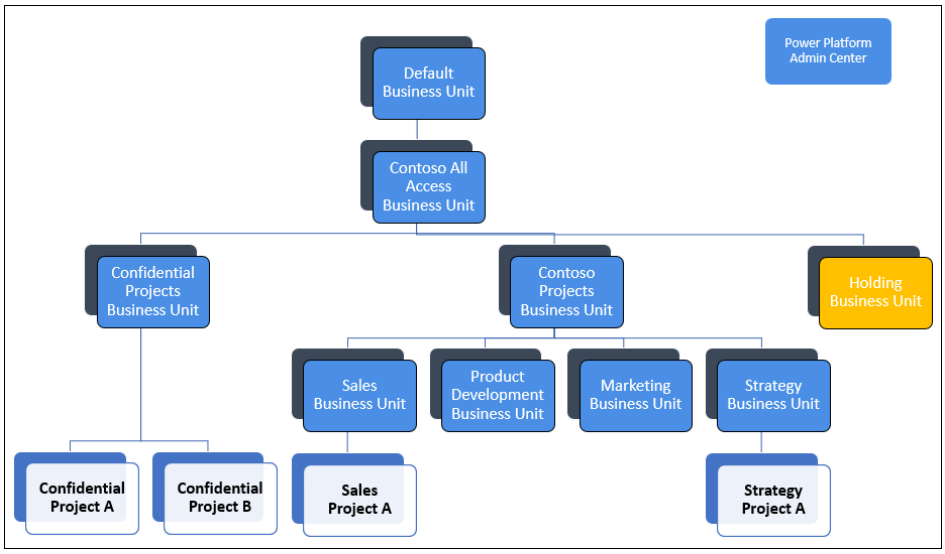
After setting up your organization's top-down Portfolio Security model, you may find the need to provide access to specific projects for some users outside the configured access boundaries. This can be accomplished with the project security option (in conjunction with portfolio security) which provides this capability. For more information see Project Security & Access.

Example: Portfolio & Project Access by Exception Using Holding Pool without Confidential Projects Business Unit



- A select group of users are given membership in an All Access business unit.
- Majority of users placed in a Holding Pool business unit that has no portfolio, program, or project access. These users are given access to either a portfolio or to individual project by exception, as needed.

Example: Portfolio & Project Access by Exception Using a Holding Pool with a Confidential Projects Business Unit



- A select group of users are given membership in an All Access business unit.
- A select group of users are given membership in a Confidential Projects business unit for additional granularity.
- A select group of users are given access to a somewhat less restrictive group of projects (Contoso Projects business unit).
- Majority of users are placed in a Holding Pool business unit that has no portfolio, program, or project access. These users are given access to either a portfolio or to individual project by exception, as needed.

Portfolio Security Configuration Steps

Tip If you need to manage project access for individual users by exception **after** setting up Portfolio Security, see Project Security & Access.

Note

- Only users with the System Administrator security role can manage business units and security roles in the BrightWork 365 environment.
- Customers that want their custom tables to be included in the Project move Program and Program move Portfolio flows will need to request assistance from their Customer Success Partner to update the child flows in their custom solution.

Caution Before proceeding:

- Confirm that Modern business units have been enabled in the BrightWork 365 environment as described in the BrightWork 365 Install Guide.pdf and BrightWork365 Upgrade Guide.pdf
- Have a clear understanding of the business unit and portfolio hierarchy that you want to create, which business unit users will reside in, and the security roles they will be given in their home business unit and in other business units if you plan to provide some users with extra access.

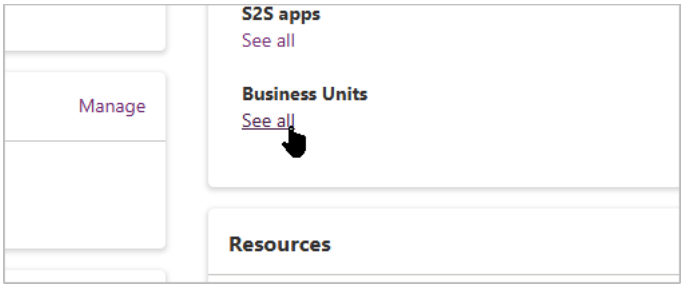
Prerequisite Step: Design your organization's security access hierarchy

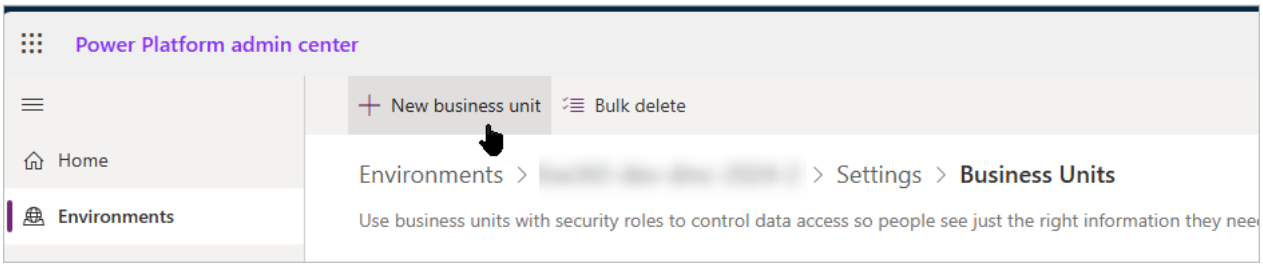
Prior to physically implementing a security access hierarchy and configuration, map out the design 'on paper' along with an analysis of practical implications and future needs.

Step 1: Create an all-access parent business unit for users that need access to all app records, i.e., "{org name} All Access"

This step is a best practice for future design flexibility.

1. Login to the https://admin.powerplatform.microsoft.com/environments and select your environment.
2. Click **Business Units > See all** and **+ New business unit**.

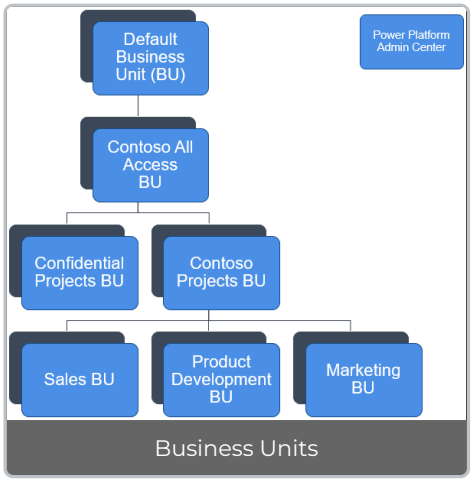




3. Fill out the form - pay attention to the Parent business unit that you select.
4. Click **Save**.

Step 2: Create a business unit hierarchy under your All Access business unit

> **Note** Child business units inherit user security role assignments from their parent business units.



- Business units are created in the Power Platform Admin center by a System Admin.
- All business units, apart from the Default Business Unit, have a parent business unit.
- New business units get non-editable copies of all the security roles found in the automatically created environment Default Business Unit (e.g., all the security roles that ship with BrightWork 365).

- Setting the Owning Business Unit in a Portfolio sets what child users will see or not see.
- Portfolios are the top-level grouping for Projects.
- Programs are a second-level grouping for projects.

Step 3: Assign users to a home business unit

Caution

- A user with the BrightWork PMO security role will have organization-wide global access regardless of their assigned business unit. They will have access to all content within BrightWork 365 including confidential projects.
- If a user's business unit is changed, all of their security roles are removed from all business units. They will need to be reassigned all of their security roles in the new business unit. Take note of their current security role assignments prior to any business unit change.

Assigning users to a home business unit will in turn control which portfolios, programs, and projects they have access to. Users will retain their current access level to individual projects after they are assigned to a business unit - a user's project access level can be viewed on the project's Team Tab. For more information see Project Security & Access.

Note

- It can take 30-60 seconds per user when their business unit is changed using the admin center Modern UI.
- User business unit assignments can be viewed in person views in the Admin Area.

In the **Microsoft Power Platform admin center:**

1. Select the BrightWork 365 environment.
2. Navigate to **Settings > Users + permissions**.
3. Select **Users**.
4. Select the relevant user.
5. On the action bar at the top of the screen select **Change business unit**.
6. In the Change business unit pane, select a business unit (do not select the option to move records to the new business unit).
7. Select **OK**.

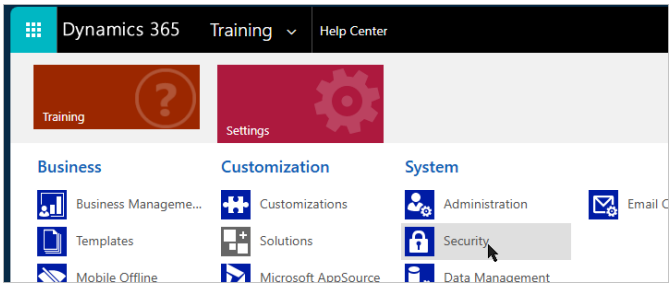
Step 4: Assign security roles to users in their home business unit

> **Note**
> - Users will display as a choice option in the various app user drop-down fields even if they have not been given any access to the project, program, or portfolio.
> - If you want to assign a user security roles in more than one business unit (giving them the same security role in each), you should do so individually, not in bulk.

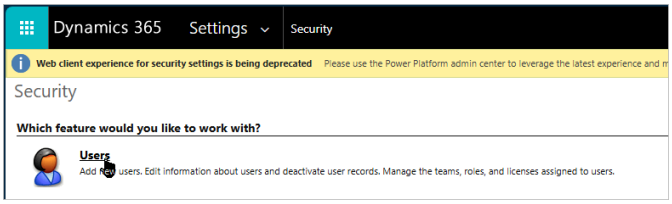
Option 1: Assign security roles to users in bulk

User security roles can be assigned in bulk via the legacy Dynamics view by the environment administrator. Note this bulk option is being phased out by Microsoft and will not always be available.

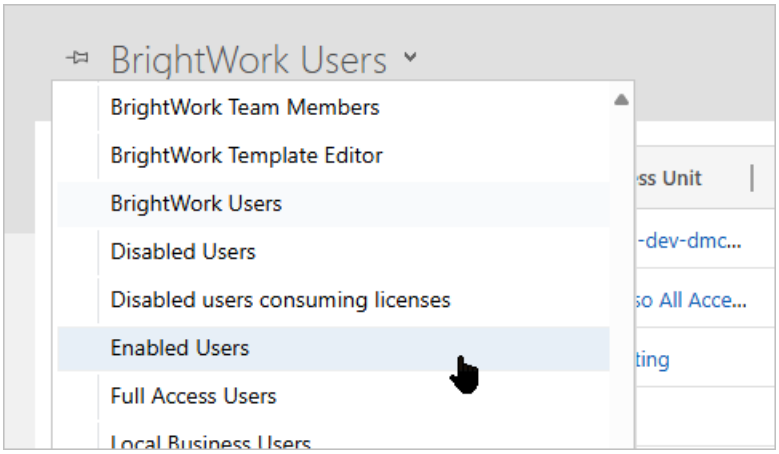
1. Login to your BrightWork 365 app and append ?forceclassic=1 after the main.aspx in the URL, e.g., https://bw365.crm4.dynamics.com/main.aspx?forceclassic=1
2. Expand the menu and click **Settings > Security**.



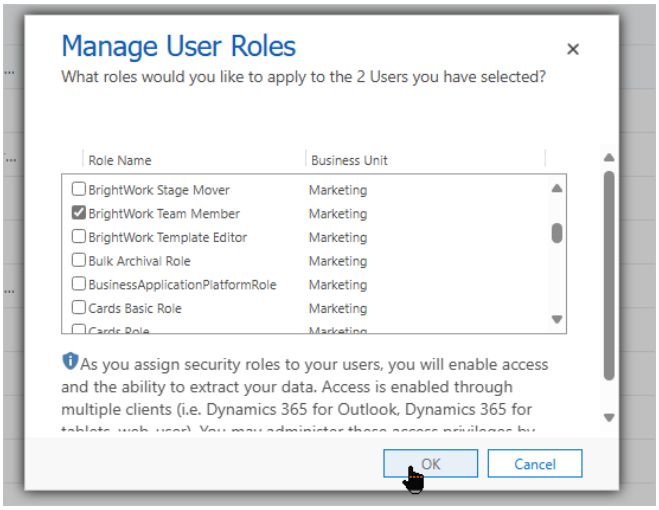
3. Click **Users**.



4. Change the view from BrightWork Users to Enabled Users.



5. Select the users you want to apply the same security role to and select **Manage Roles**.
6. Select the roles that you want to assign and click **OK**.



Option 2: Assign security roles to users individually

In the **Microsoft Power Platform admin center:**

1. Select the BrightWork 365 environment.
2. Navigate to **Settings > Users + permissions** .
3. Select **Users**.
4. Select the relevant user.
5. On the action bar at the top of the screen click **Manage security roles**.
6. Confirm the business unit selection.
7. Select the **Basic User** and **BrightWork Team Member** security roles (at a minimum), and any other desired security roles the user needs.
8. Click **Save**.

Step 5: (Optional) Assign security roles to users in secondary business units as needed

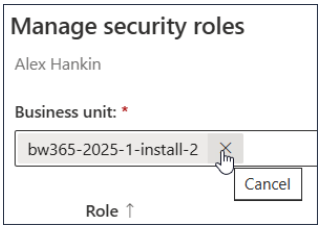
Users can only be a member of one business unit but can be given the same security role they have in their home business unit in other business units to broaden their access to portfolios, programs, and projects.

> **Caution** Users assigned security roles in secondary business units must be given the same security roles that they've been given in their home business unit.

For example, Alex is a BrightWork Project Manager in Marketing, which is his home business unit. He can also be given the BrightWork Project Manager security role in the secondary Product Development business unit.

In the **Microsoft Power Platform admin center:**

1. Select the BrightWork 365 environment.
2. Navigate to **Settings > Users + permissions** .
3. Select **Users**.
4. Select the relevant user.
5. On the action bar at the top of the screen click**Manage security roles**.
6. Clear the existing business unit entry.



7. Search for the relevant secondary business unit and select it.
8. Assign all of the security roles that the user has in their home business unit, e.g., Basic User, BrightWork Team Member, BrightWork Project Manager.
9. Click **Save**.

Step 6: Create portfolios that will act as the top parent levels of the hierarchy in BrightWork 365 (Portfolios > Programs > Projects)

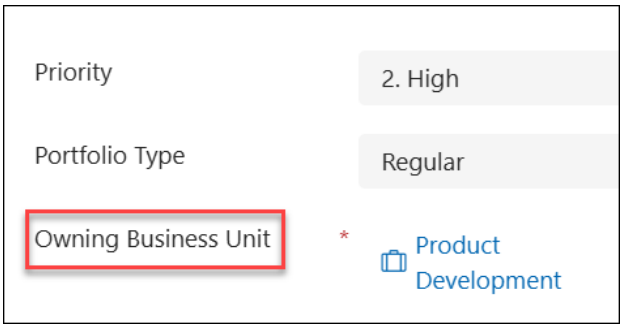
See Portfolios for details.

Step 7: Select an Owning Business Unit within each Portfolio

> **Note**
> - Only users with the BrightWork PMO Manager or System Administrator security role can configure a Portfolio's Owning Business Unit.
> - A business unit can own as many portfolios as necessary.
> - If a Portfolio's Owning Business Unit is changed to one that is above its current Owning

Business Unit in the hierarchy, the change will be automatically reversed, and an email notification of this reversal will be sent to the person who attempted the change
- The Change Owning Business Unit dialog in Portfolios can take a few seconds to open, depending on the number of records (Programs and Projects) it has to check.
- When the Owning Business Unit is selected, the amount of time it takes for the value to propagate to all child records is related to the number of Portfolio child records. When the process is complete, an email notification will be automatically sent to the Portfolio Manager and the user that made the selection.

1. In the Portfolio's **Statement** tab, select the relevant Owning Business Unit in the **Owning Business Unit** field.



2. Read the warning message, choose the new Owning Business Unit, and click **Confirm** or **Cancel**.

Caution

- If the Owning Business Unit of a Portfolio is changed, the Owning Business Unit of all the child Program and Project related records will also be updated. This means that some users in the previous business unit may lose access to this portfolio and the other records. It also means that users in the new Business Unit will now be able to access records in this Business Unit.
- Concurrent usage is not supported, e.g., before moving a Portfolio's Owning Business Unit, the BrightWork PMO Manager should inform the team to exit any child Projects of the Portfolio.

Step 8: Assign programs to a parent portfolio associated with the business unit desired for the program and its child projects

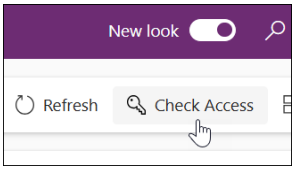
Programs inherit the Owning Business Unit from their parent portfolio.

To associate a program with a parent portfolio, select the relevant portfolio as you normally would in the program's **Statement** tab.

> **Note** If a program is moved to a different portfolio with a different associated business unit, or if a portfolio's associated business unit is changed, some users who never had access to that part of the hierarchy will now have access, and some that had access previously will no longer have access; this will be determined by either their own business unit, or from access granted at the project level.

Check User Access

1. Navigate to the Portfolio or Program and click the **Check Access** button in the toolbar.



2. Click the **Who has access** link to see information about all users that have access to the project
3. You can click the **User details** button for a user to view a report that tells why the user has access.

Security and Power BI Reports

BrightWork 365 supports Row Level Security in Power BI reports with some caveats that you should be aware of. These caveats are outlined below.

BrightWork 365 ships with 4 Power BI reports:

- My Work
- Resource Utilization
- Portfolios 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 after the report 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

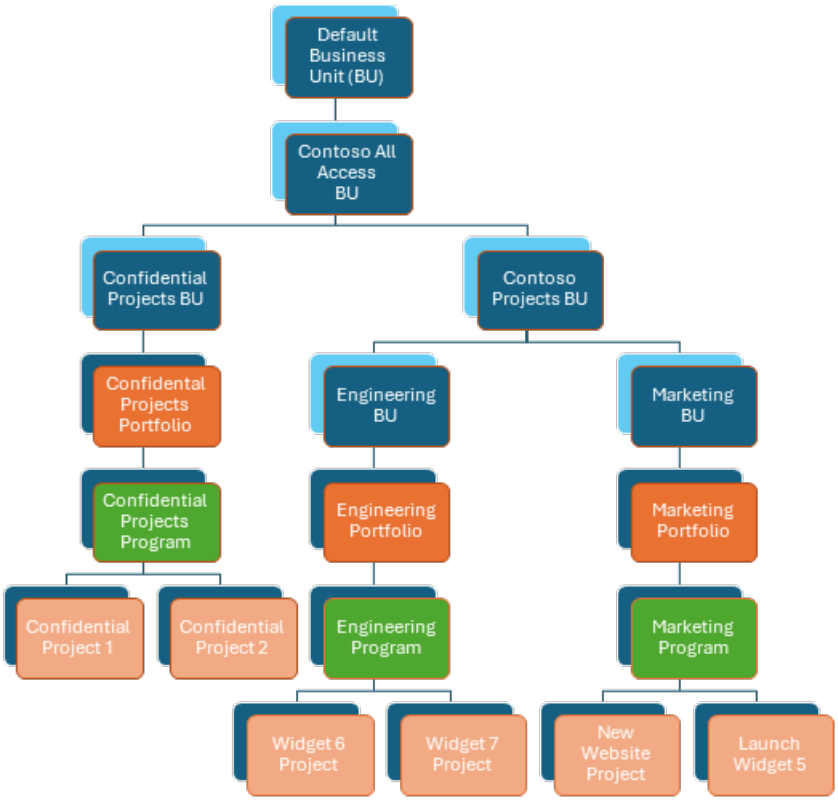
The Resource Utilization is designed to enable project managers assess the availability of users in the organization for work. As such, it should be a global report.

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 business unit security is enabled by setting the enforcement of Row Level Security (RLS) to True in the Power BI report (see the Implementing Business Unit Security section below). 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 down 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

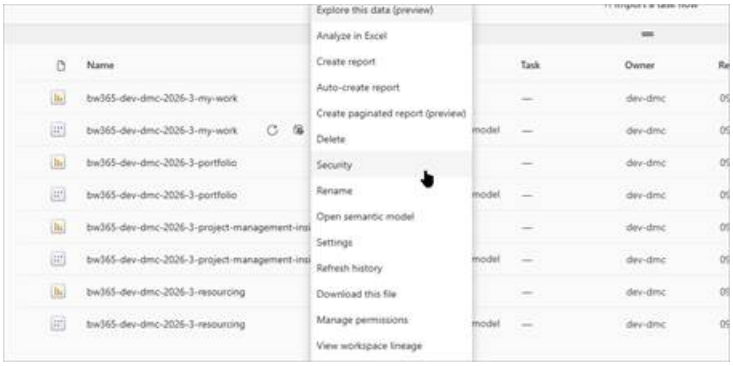
The Project Management Insights report is designed as a BrightWork PMO Manager only report.

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.

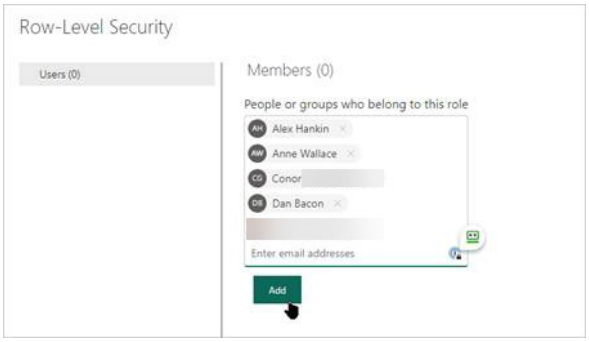
Giving Users Report Access

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.



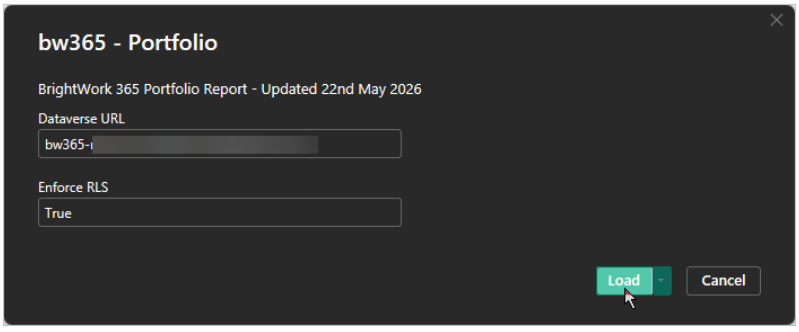
3. Add each user who will be accessing the report, click **Add**, and click **Save** when done. You can also add a team in which the users are a member.



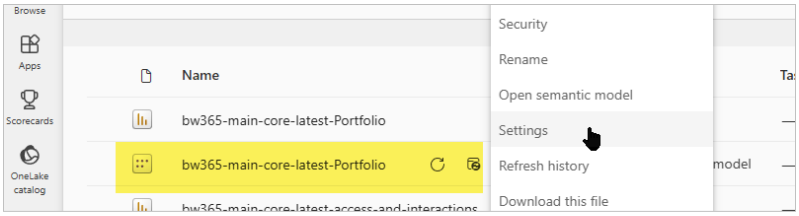
Implementing Business Unit Report Security

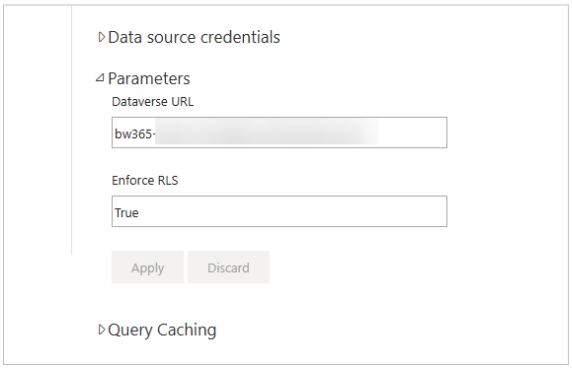
Business Unit report security can be implemented for the Power BI reports that support it (see the Security and Power BI Reports section above), by choosing to Enforce Row Level Security (RLS) when setting up the Power BI PBIT.

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:


Browse
Apps
Scorecards
OneLake catalog
Name
bw365-main-core-latest-Portfolio
bw365-main-core-latest-Portfolio
Security
Rename
Open semantic model
Settings
Refresh history
Download this file
model


Data source credentials
Parameters
Dataverse URL
bw365-
Enforce RLS
True
Apply
Discard
Query Caching