Project Security & Access

Project Management Context

Organizations are not always able 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 options to accommodate both of these approaches through a flexible security and access model.

One of the available BrightWork 365 security models is the Portfolio Security model, which limits access to only those users given a BrightWork security role in a portfolio's associated Owning Business Unit. This top-down access for users (or lack thereof) propagates through the portfolio's hierarchy to the project level. However, user access exceptions will often need to be made, for example to allow team members access to a child project even though they are not given any security role at the parent portfolio level. In these instances, after you implement the Portfolio Security model, you can then proceed to use the Project Security Model detailed in this article to allow users access to individual projects to which they would otherwise not have access.

Your browser does not support HTML5 video.

Note

- When projects are first created, their Owning Business Unit, which affects which users have access, will be inherited from their parent Portfolio (see Portfolio Security & Access).
- For Projects created from content templates, their Owning Business Unit will be taken from the source project.
- If a user does not have any access to a Project, Program, or Portfolio by any method, they will still display as a choice option in user drop-down fields.
- Customers that wish their custom tables to be included in the Project Move, Program Move,

and Portfolio Move flows will need to request assistance from their Customer Success Partner to update the child flows in their custom solution.

Caution

- Customers are advised to use generic names for planned confidential projects as the project names will be visible to all users in various places in the app and in Power BI / SharePoint (Approvals, Content Templates). Confidential projects should not contain confidential information in their project name.
- Users with the BrightWork PMO Manager or System Administrator security role automatically get access to everything in BrightWork 365.
- Security & Access functionality will not work if you have customized BrightWork 365 out of the box Security Roles. If necessary, create and use custom security roles instead.

What's In 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 • Microsoft Teams • Requests • Content Templates

---

Project Security Configuration Steps

Prerequisite: Confirm that portfolio security has been fully configured

- See Portfolio Security & Access for details.

Step 1: Set the Default Access Level in Project Templates

1. Click into **Templates Area > Project Templates**.
2. Select a project template.
3. In the **Details tab > New Project Defaults** section choose a **Default Access Level** of **Edit** or **None**.
4. Click **Save & Close**.

Step 2: Create Project

See Create Projects for project creation details.

Step 3 (Optional): Change the Project's Default Access Level

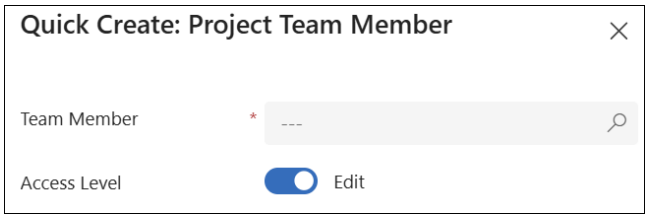
The project's Default Access Level is inherited from its associated project template. To change the project's Default Access Level:

1. In the project's Charter tab or Project Settings tab click the link in the Schedule Settings field.
2. Click the Project Settings tab and select the desired Default Access Level.
3. Click **Save & Close**.

Step 4: Add Project Team Members

Project team members can be added to a project by a user with a relevant security role in a couple of ways:

- Assign work to a user, e.g., Gantt task, Risk, Issue, Action. After being assigned to work the user will be added to the project Team tab.
- In the project **Team** tab, click **New Project Team Member**, choose the user and select an **Access Level** for them (this is only relevant for individual team members that do not automatically have access via a security role and business unit associated with the project). The Access Level value for the project team member record determines the access that the user has in the project.



  - If you remove assignments from a team member, they still have their access to the project. If you delete them from the project's Team tab they will then lose their access to the project assuming they don't also have access via a business unit security role.
  - When a project moves to a different program/portfolio the user's project access level moves with them to the new portfolio.
  - When a user is made the actual Project Manager of a project, they will automatically be given the Edit access level for the project regardless of the Default Access Level setting. The Project Manager field in a project is populated with all users that have been given the BrightWork Project Manager security role, irrespective of any business unit provided access or lack thereof. If subsequently the actual Project Manager is changed to someone else, the prior actual Project Manager will retain their Edit access so that they will not get locked out of the project if it is in a business unit in which they don't have any security roles.
  - The Access Level for users with the BrightWork PMO Manager security role must be set to Edit; if an attempt is made to change their Access Level it will be reset to Edit and an email explaining this change will be sent to the actual project manager of the project.
  - The Approval Coordinator and Project Sponsor (from outside the project's Business Unit) need to be manually added as project team members and given the desired Access Level. Approvers can approve via email and are not required to have an Access Level of Edit.

Step 5 (Optional): Override the project's Default Access Level by exception to Edit or None for existing team members

This is only relevant for individual team members that do not have security role access to the project. The Access Level value for the project team member record determines the access that the user has in the project.

1. In the project's **Teams** tab, click the name of the relevant user.
2. Set the **Access Level** to **None** or **Edit**.



Note

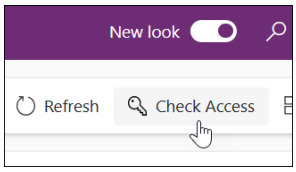
- Only the actual Project Manager of a project and users with the BrightWork PMO Manager security role can edit a project team member's Access Level.
- When a security role is granted to a user after they are added to the Team tab in a project, and that user had an Access Level of None prior to being given the security role, the Access Level will continue to display as None even though the user now actually has Edit access.
- Users cannot access the parent Program and Portfolio in which the Project they were given access to is located, unless they also have access through standard business unit membership. See Portfolio Security & Access for more information.

Caution

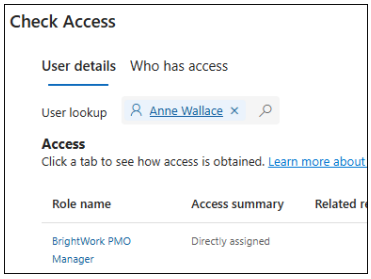
- The actual Project Manager of the project always gets access to the project. Therefore, if you want to setup a confidential project but not let the project manager have access to it yet, make yourself the project manager until you are ready to let the planned project manager know about the project.
- When a Team Member is deleted from a project's Team tab, this does not revoke access for the user, and they will still have access to the project unless the project is a confidential project.

Check User Project Access

1. From within a project, select the **Check Access** link in the toolbar of the Project.



2. Search for the relevant user in the **User lookup** field and view their project access details.



3. Click the **Who has access** link to see information about all users that have access to the project.