User Management

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

Definitions

- **Security:** Methods for protecting the system as a whole and the data housed within the system. Security is cumulative.
- **User Security:** Defines user access to Tables, Columns, Rows, etc., in the Power Platform Dataverse. Individual user access is controlled through an accumulated combination of their associated Security Roles, Business Unit, Dynamics Teams, etc. Users will get the least restrictive combination of all their security roles.
- **Security Role**: Defines permission to Tables and other miscellaneous privileges.

Add Users to the Power Platform Environment

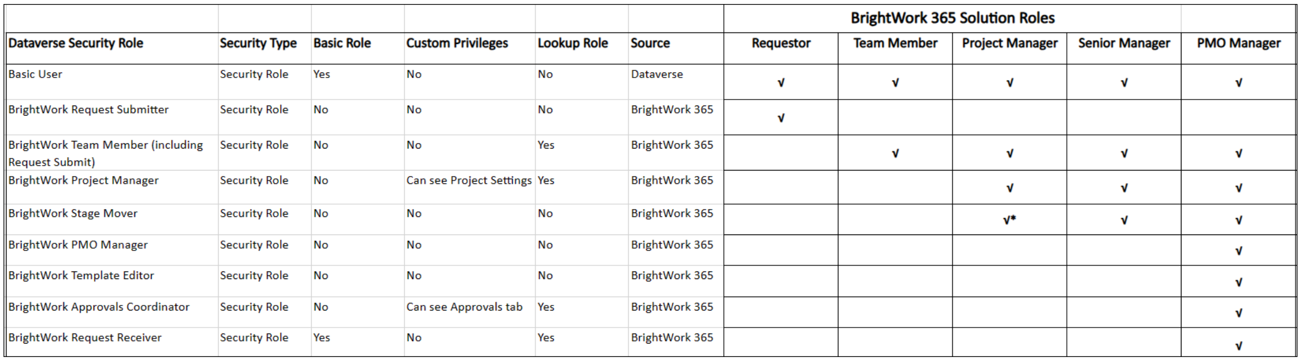
Microsoft 365 admins will need to first give users access to the Power Platform environment that contains the BrightWork 365 solution; this can be done either individually or with the recommended method of adding users to a Microsoft 365 Security Group (Microsoft article) that is part of the environment. If no users at all are added to the environment then all Active Directory users will have environment access.

Security groups can be created either directly within the Microsoft 365 admin center, or through the creation of a private Microsoft Team which will in turn automatically create a security group with the same given name in Microsoft 365. Once the security group is created, users can be added to it either via the Microsoft 365 admin center or by adding them to the Microsoft Team.

Once a user is added to the environment, an environment System Administrator must assign security roles to the user so they may use the BrightWork 365 app in the intended manner - see the **Security Roles** sections below.

For additional details about controlling user access to Power Platform environments, Entra ID (formerly known as Azure Active Directory) security groups, and licensing, see this Microsoft documentation and contact your organization's system administrator.

Assign Security Roles to Users



						BrightWork 365 Solution Roles				
Dataverse Security Role	**Security Type**	**Basic Role**	**Custom Privileges**	**Lookup Role**	**Source**	**Requestor**	**Team Member**	**Project Manager**	**Senior Manager**	**PMO Manager**
Basic User	Security Role	Yes	No	No	Dataverse	√	√	√	√	√
BrightWork Request Submitter	Security Role	No	No	No	BrightWork 365	√				
BrightWork Team Member (including Request Submit)	Security Role	No	No	Yes	BrightWork 365		√	√	√	√
BrightWork Project Manager	Security Role	No	Can see Project Settings	Yes	BrightWork 365			√	√	√
BrightWork Stage Mover	Security Role	No	No	No	BrightWork 365			√*	√	√
BrightWork PMO Manager	Security Role	No	No	No	BrightWork 365					√
BrightWork Template Editor	Security Role	No	No	No	BrightWork 365					√
BrightWork Approvals Coordinator	Security Role	No	Can see Approvals tab	Yes	BrightWork 365					√
BrightWork Request Receiver	Security Role	Yes	No	Yes	BrightWork 365					√

In addition to adding users to the overall Power Platform environment as noted above, users will also need to be granted **security roles** after importing the BrightWork 365 solution. Security roles need to be assigned to users individually (not through the use of Entra ID (formerly known as Azure Active Directory) security groups), and this is done through the standard Power Platform role assignment process. You can also bulk assign security roles to multiple users with the User Roles Manager utility in XrmToolBox.

See the **BrightWork Security Roles Details** article for an explanation of the various security roles; for more granular details see the spreadsheet BrightWork 365 Security Roles.xlsx

Basic User: All BrightWork 365 users must be assigned this security role in addition to any other security roles they may also be assigned.

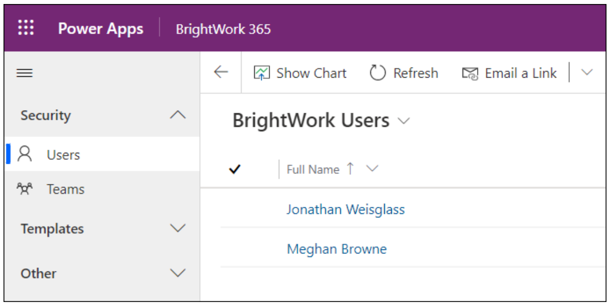
BrightWork Request Submitter: If a user will be given a free BrightWork 365 license to be able to only submit project requests, they will also require this security role.

Note

- In addition to the free BrightWork 365 license, these users will also need a paid MS Power Apps license.
- Although this limited user will only see the Requests area on the main nav, they still have access to other app areas through alternate navigation such as by clicking on linked columns, e.g., the **Program** column in the **Request** form.

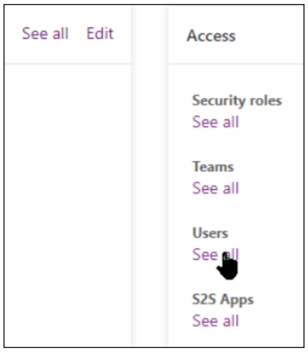
All **paid license** BrightWork 365 users at a minimum need the following security role in addition to **Basic User**:

- **BrightWork Team Member:** This security role consumes a BrightWork 365 license and is not for those users who will only be **Request Submitters** as noted above. Users granted the **BrightWork Team Member** security role will appear in the app's **Admin Area** in **Security > Users > BrightWork Users**.

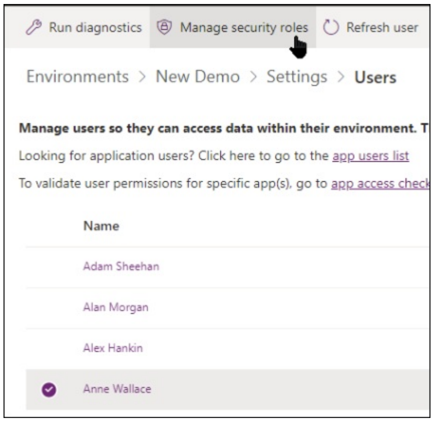


To assign security roles to users individually:

1. Login to your organization's Power Platform admin center and click the environment where you installed BrightWork 365.
2. Click **See all** under Users.



3. Select a user and click **Manage security roles**.



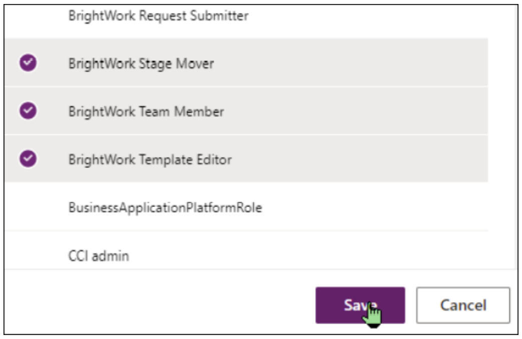
Manage users so they can access data within their environment. T

Looking for application users? Click here to go to the app users list

To validate user permissions for specific app(s), go to app access check

Name
Adam Sheehan
Alan Morgan
Alex Hankin
Anne Wallace

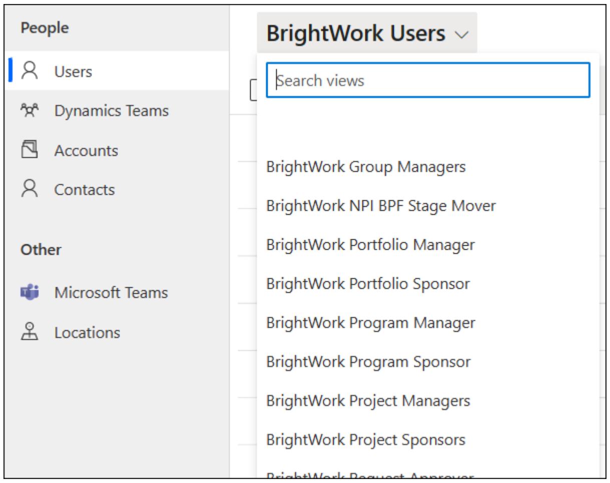
4. Select the roles you want to apply to the user and click Save.


BrightWork Request Submitter
BrightWork Stage Mover
BrightWork Team Member
BrightWork Template Editor
BusinessApplicationPlatformRole
CCI admin
Save
Cancel

> **Note** If security role changes are made to a user that is already logged in to the app, the user will need to either refresh the screen with Ctrl-F5 or log out of the BrightWork 365 app and log back in to utilize the security role changes.

View Current Security Role Assignments In-App

1. Go to the Admin Area.
2. Click on the Users table link in People section of the Site Map.
3. Click the drop-down arrow to view users assigned to the various security roles.


People
Users
Dynamics Teams
Accounts
Contacts
Other
Microsoft Teams
Locations
BrightWork Users
Search views
BrightWork Group Managers
BrightWork NPI BPF Stage Mover
BrightWork Portfolio Manager
BrightWork Portfolio Sponsor
BrightWork Program Manager
BrightWork Program Sponsor
BrightWork Project Managers
BrightWork Project Sponsors

Create the Senior Managers Dynamics Team

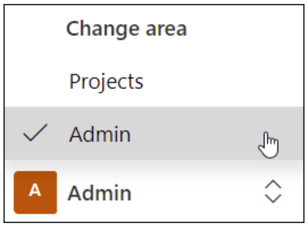
The BrightWork 365 Senior Managers Dynamics Team is used to limit the users that are able to view cost and budget data for portfolios and programs, and to define the users returned in the following lookups:

- Group Manager
- Portfolio Manager
- Portfolio Sponsor

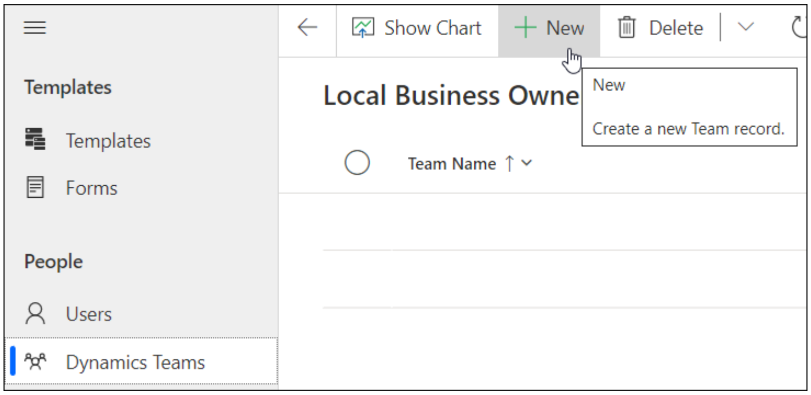
- Program Manager
- Program Sponsor
- (Request) Reviewers
- (Request) Approvers

To create the Senior Managers Dynamics Team and add users:

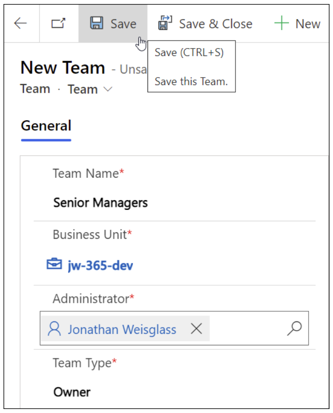
1. Login to the BrightWork App.
2. Switch to the **Admin** area.



3. Click **Dynamics Teams** and click **+ New.**



4. Name the team "**Senior Managers**".
5. Select a **Business Unit**, make yourself the Administrator and click **Save**.



Team Name*
Senior Managers

Business Unit*
jw-365-dev

Administrator*
Jonathan Weisglass

Team Type*
Owner

6. Click **Add Existing User** to begin adding your users to the team.

> **Note** It is possible to more granularly limit the users returned in the lookup columns

> noted above beyond what is offered by the Senior Managers team with the use of additional lookup column security roles and related configuration changes. For more detailed information contact your BrightWork Customer Success Partner.

Remove User Access to BrightWork 365

If you need to remove user access to BrightWork 365, the recommended approach is to disable the relevant user accounts.

Do not delete the disabled user accounts nor remove their security roles from the BrightWork 365 environment. Doing so will cause issues such as flow failures, maintaining historical context, preventing the successful updating of the Owning Business Unit of Portfolios, moving Projects to different Programs, and moving Programs to different Portfolios. If related issues are encountered:

- Add the missing BrightWork Security Roles back to the disabled user (the user can remain disabled if desired) or,
- Delete all assignments associated with these disabled users, remove them from all lookups (especially Project Manager), and then delete their associated Project Team Member records.

Troubleshooting

User Access Issues

With user diagnostics you can run through a series of checks to determine the health of a user account and view recommendations for resolving issues.

1. Navigate to the Power Platform admin center, Environment Details page.
2. Click on Settings | Users.
3. Select the user and choose Run diagnostics from the top of the screen.
4. Check the diagnostic Status and Results notes for any issues and resolution recommendations.

Practical Exercise

Draft the user management strategy for your group to start and for your anticipated future needs.