P10: Managing Users in Power Platform Admin Center

Friday, April 18, 2025 8:19 PM

Context

Item	Detail
Tag	Vertical Patterns | Power Platform Admin Center
Contributors	Vincent Kimiti
Version Control	V1.0
Application Use Case	Manage user access, permissions, and security roles in a Power Platform environment
Reference Usage	Administering user access in Power Platform environments

Story Behind The Pattern

Item	Detail
The Problem	Managing user access in Power Platform environments can be complex, leading to unauthorized access or insufficient permissions for users.
The Solution	Use the Power Platform Admin Center to add, remove, and manage users, validate their permissions, and assign appropriate security roles.
Dependencies	Power Platform Admin Center access for user management, permissions to manage environments and security roles.

The Pattern

Method: Managing Users in Power Platform Admin Center

Here's a step-by-step guide to manage users, their permissions, and security roles in the Power Platform Admin Center:

1. Access the Power Platform Admin Center
    - Log in to the Power Platform Admin Center (admin.powerplatform.microsoft.com) using your admin credentials.
    - Navigate to the environment where you want to manage users (e.g., "DQ FACTORY - DFSA - Primary DEV") by selecting it from the environment list in the top-right corner.

2. View the User List
    - In the selected environment, go to the Users section (typically found under the main section or in the sidebar under "Settings").
    - Review the list of users who can access data within the environment.
    - Check the columns for Name, Username, and Email to identify users.

3. Add a New User
    - Click the Add user button to open the pop-up window.
    - Enter the user's name or email address in the search field to find them in Microsoft Entra ID.
    - Verify that the user meets the access requirements:
        - The user must be enabled in Microsoft Entra ID.
        - The user must be a member of the environment's security group (if applicable).
    - Select the user from the search results and click Add to include them in the environment.

- Confirm the user appears in the user list with the correct details.

4. Remove a User
   - Navigate to the Groups list within the environment (this may be under "Settings" or "Security").
   - Select the user you want to remove from the list.
   - Follow the prompts to remove the user from the environment (e.g., click "Remove" and confirm the action).
   - Verify the user no longer appears in the user list.

5. Validate User Permissions
   - Go to the App Users section within the environment (often under "Apps" or "Security").
   - Select a user to check their permissions for specific applications.
   - Review the assigned permissions and make adjustments if necessary (e.g., grant access to additional apps or restrict access as needed).
   - Save any changes to ensure the user has the correct access.

6. Navigate Using the Sidebar
   - Use the sidebar on the left to access different sections of the Power Platform Admin Center:
     - Home: Overview of the admin center.
     - Environments: Manage different environments.
     - Data: Manage data integrations.
     - Solutions: View and manage solutions.
     - Apps: Manage applications.
     - Analytics: Access usage and performance reports.
     - Settings: Configure environment settings, including user management.
   - Use these sections to explore additional user management options if needed.

7. Manage Security Roles
   - From the user list, select the user for whom you want to manage security roles.
   - Click Manage security roles to open the pop-up window.
   - Assign the appropriate roles from the list (e.g., "Activity Feeds," "App End User," "Analytics Report Author").
   - Remove any roles that are not required by unchecking them.
   - Click Save to apply the changes.
   - Verify the updated roles by checking the user's permissions in the environment.

8. Test and Validate Changes
   - Log in as the user (or use a test account) to confirm they have the expected access and permissions.
   - Test specific actions (e.g., accessing an app, viewing data) to ensure the security roles are correctly applied.
   - If issues arise, revisit the user's permissions or security roles and adjust as needed.