P14: Managing Security Roles 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 security roles to control user access and permissions in a Power Platform environment
Reference Usage	Administering security roles for data security and compliance in Power Platform

Story Behind The Pattern

Item	Detail
The Problem	Improperly managed security roles can lead to unauthorized access, data breaches, or users lacking necessary permissions to perform their tasks.
The Solution	Use the Power Platform Admin Center to view, assign, create, and modify security roles, ensuring proper access control and compliance.
Dependencies	Power Platform Admin Center access, permissions to manage environments and security roles, Microsoft Entra ID for user authentication.

Introduction to Security Roles

Security roles in Power Platform and Dynamics 365 are used to control access to data and resources within an environment. They define what actions users can perform and what data they can access based on their assigned roles. Security roles are essential for maintaining data security, ensuring compliance, and managing user permissions effectively.

The Pattern

Method: Managing Security Roles in Power Platform Admin Center

Here's a step-by-step guide to manage security roles in the Power Platform Admin Center, including viewing, assigning, creating, and modifying roles:

1. Access the Power Platform Admin Center
    - Log in to the Power Platform Admin Center (admin.powerplatform.microsoft.com) using your admin credentials.
    - Ensure you have the necessary permissions to manage environments and security roles.

2. Navigate to Environments
    - Use the navigation menu on the left sidebar to go to the Environments section.
    - Select the environment where you want to manage security roles (e.g., "DSFA - DEV - REBUILD A").

3. View Security Roles
    - In the selected environment, go to Settings in the sidebar.
    - Navigate to Users + Permissions > Security roles.
    - Review the list of predefined security roles (e.g., System Administrator, Environment Maker) and any custom roles that have been created.

- Note the privileges associated with each role to understand their scope.

4. Assign Security Roles to Users
   - Navigate to the Users section within the environment (under Users + Permissions).
   - Select a user from the list of users in the environment.
   - Click Manage security roles to open the pop-up window.
   - Assign the appropriate roles to the user by checking the boxes next to the desired roles (e.g., "System Administrator," "Environment Maker").
   - Remove any unnecessary roles by unchecking them.
   - Click Save to apply the changes.
   - Verify the updated roles are reflected in the user's profile.

5. Create or Modify Security Roles
   - To create a new security role:
     - Click New in the Security roles section.
     - Define the role's Name (e.g., "Sales Manager").
     - Set the privileges for the role by selecting permissions for each table and task (e.g., Read, Write, Create for the Account table; Export to Excel for tasks).
     - Save the new role.
   - To modify an existing role:
     - Select the role from the list (e.g., "Environment Maker").
     - Update its privileges as needed (e.g., add Write access to a specific table or enable a task like "Publish Articles").
     - Save the changes to apply the updated role.
   - Ensure the role aligns with your organization's access control policies.

6. Test and Validate Permissions
   - Log in as a user with the assigned or modified security role (or use a test account).
   - Validate that the user has the correct access and permissions:
     - Check data access (e.g., can the user view/edit records in the Account table as expected?).
     - Test task-based permissions (e.g., can the user export data to Excel or activate a business rule?).
     - Verify environment-level access (e.g., can an Environment Maker create new resources?).
   - If issues arise, revisit the security role settings and adjust privileges as needed.