Guynes Daniel M (Contractor)

[Email address]

Abstract

This document will provide the standard operating procedures for Power Platform Admins to implement, maintain, and implement governance across the Power Platform environment.

Power Platform Standard Operational Procedures

SOPs for Power Platform governance

Table of Contents

[Summary of Procedures and Steps 4](#_Toc190887503)

[How to Create Security Groups for Power Platform 7](#_Toc190887504)

[Security Group Naming Conventions 8](#_Toc190887505)

[Microsoft Entra Security groups 9](#_Toc190887506)

[Attaching the Entra Security Group to a Power Platform Team 13](#_Toc190887507)

[Add Security Roles to the Teams 14](#_Toc190887508)

[How to Add a Development And Sandbox Environment 16](#_Toc190887509)

[Summary of Steps: 16](#_Toc190887510)

[Step 1: Create User Security Group 16](#_Toc190887511)

[Step 2: Create Environment 16](#_Toc190887512)

[Step 3: Settings 17](#_Toc190887513)

[Step 4: Add to Proper Policy 23](#_Toc190887514)

[Step 5: Create Approval Tables 24](#_Toc190887515)

[How to Add a Production And Test Environment 26](#_Toc190887516)

[Summary of Steps: 26](#_Toc190887517)

[Step 1: Create User Security Group 26](#_Toc190887518)

[Step 2: Create Environment 26](#_Toc190887519)

[Step 3: Settings 27](#_Toc190887520)

[Step 4: Add to Proper Policy 32](#_Toc190887521)

[Step 5: Create Approval Tables 32](#_Toc190887522)

[How to Find and Replace the Owner of a Power App 35](#_Toc190887523)

[Find the Power App ID 35](#_Toc190887524)

[Power Platform Pipelines 36](#_Toc190887525)

[Summary of Steps: 36](#_Toc190887526)

[How to Create a Pipeline Host 37](#_Toc190887527)

[Summary of Steps 37](#_Toc190887528)

[Step 1: Ensure the Pipeline objects are Set 37](#_Toc190887529)

[Step 2: Create the Host Environment 37](#_Toc190887530)

[Step 3: Add Dynamics 365 apps to the Host environment. 38](#_Toc190887531)

[How to Create a Pipeline 40](#_Toc190887532)

[Summary of Steps 40](#_Toc190887533)

[Step 1: Open the Host Power Platform 40](#_Toc190887534)

[Step 2: Add Environments 40](#_Toc190887535)

[Step 3: Create New Pipeline 42](#_Toc190887536)

[Step 4: Associate the Pipeline with the Sandbox Environment 43](#_Toc190887537)

[Step 5: Create the Deployment Stages (Sandbox to Test) 44](#_Toc190887538)

[Step 6: Create the Deployment Stages (Test to Prod) 45](#_Toc190887539)

[Step 7: Setup Security for Pipelines 45](#_Toc190887540)

[How to Change the Owner of a Power App or Power Automate Flow 50](#_Toc190887541)

[Summary of Steps 50](#_Toc190887542)

[Step 1: Navigate to COE 50](#_Toc190887543)

[Step 2: Locate the Environment 50](#_Toc190887544)

[Step 3: Add the new Owner 50](#_Toc190887545)

[How to Find an Entra Group Attached to an Environment 52](#_Toc190887546)

[Summary of Steps 52](#_Toc190887547)

[Step 1: Navigate to Environment 52](#_Toc190887548)

[Step 2: Identify Entra Group ID 52](#_Toc190887549)

[Step 3: Find Group in Microsoft Entra 53](#_Toc190887550)

[Standard Processes 54](#_Toc190887551)

[Development Environments 54](#_Toc190887552)

[Sandbox (Group Development) Environments 54](#_Toc190887553)

[Security Groups / Teams 54](#_Toc190887554)

[Test Environments 54](#_Toc190887555)

[Security Groups / Teams 54](#_Toc190887556)

[Production Environments 55](#_Toc190887557)

[Security Groups / Teams 55](#_Toc190887558)

[Standard Reports 56](#_Toc190887559)

[Standard Operating Procedures 57](#_Toc190887560)

[COE Updates 58](#_Toc190887561)

# Table of Figures

[Figure 1 9](#_Toc190887568)

[Figure 2 9](#_Toc190887569)

[Figure 3 10](#_Toc190887570)

[Figure 4 13](#_Toc190887571)

[Figure 5 13](#_Toc190887572)

[Figure 6 13](#_Toc190887573)

[Figure 7 14](#_Toc190887574)

[Figure 8 16](#_Toc190887575)

[Figure 9 16](#_Toc190887576)

[Figure 10 17](#_Toc190887577)

[Figure 11 17](#_Toc190887578)

[Figure 12 18](#_Toc190887579)

[Figure 13 18](#_Toc190887580)

[Figure 14 21](#_Toc190887581)

[Figure 15 21](#_Toc190887582)

[Figure 16 22](#_Toc190887583)

[Figure 17 22](#_Toc190887584)

[Figure 18 26](#_Toc190887585)

[Figure 19 26](#_Toc190887586)

[Figure 20 27](#_Toc190887587)

[Figure 21 27](#_Toc190887588)

[Figure 22 28](#_Toc190887589)

[Figure 23 28](#_Toc190887590)

[Figure 24 30](#_Toc190887591)

[Figure 25 30](#_Toc190887592)

[Figure 26 31](#_Toc190887593)

[Figure 27 31](#_Toc190887594)

[Figure 28 35](#_Toc190887595)

[Figure 29 39](#_Toc190887596)

[Figure 30 39](#_Toc190887597)

[Figure 31 40](#_Toc190887598)

[Figure 32 41](#_Toc190887599)

[Figure 33 42](#_Toc190887600)

[Figure 34 42](#_Toc190887601)

[Figure 35 43](#_Toc190887602)

[Figure 36 43](#_Toc190887603)

[Figure 37 44](#_Toc190887604)

[Figure 38 44](#_Toc190887605)

[Figure 39 45](#_Toc190887606)

[Figure 40 46](#_Toc190887607)

[Figure 41 46](#_Toc190887608)

[Figure 42 47](#_Toc190887609)

[Figure 43 47](#_Toc190887610)

[Figure 44 48](#_Toc190887611)

[Figure 45 49](#_Toc190887612)

[Figure 46 50](#_Toc190887613)

[Figure 48 51](#_Toc190887614)

# Table of Tables

**No table of figures entries found.**

# Summary of Procedures and Steps

1. User requests a Sandbox (Development) Environment (Day 1) **DO WE CREATE TEST ENVIRONMENT AT THE SAME TIME?**
   1. User Action:
      1. Create IR Works Request
   2. PPT Action:
      1. Review request – speak with User – Create Environment (see How to Add a Sandbox Environment)
2. User requests one or more Security groups for their environment (Day 1)
   1. User Actions:
      1. Create IR Works Request for EACH group (include CVS for users)
         1. User Group
         2. Maker Group
   2. PPT Action:
      1. Create the groups in Entra and then in the Sandbox (Development) environment.
         1. Review request
         2. speak with User

# Create each group (see Power Platform Basics

To implement proper Power Platform application and flow development, the PPT will provide three environments as follows:

* Sandbox (Type: sandbox, unmanaged)
* Test (Type: production, managed)
* Production (Type: production, managed)

# Security for Power Platform Environments

The Power Platform Team does not provide individual access to Environments. PPT will use Microsoft Entra Security Groups to apply a role-based method for applying access to Power Platform Environments. This provides the user base with self-governance of access, while also providing Microsoft best-practice security for environments.

## Security Group Allocation

* + - 1. How to Create Security Groups for Power Platform)

1. User requests premium connectors for Sandbox (Day1)
   1. User Action:
      1. Create Change Request for Premium Connection
      2. Obtain SecCHM ID
      3. Provide that to us for documentation.
   2. PPT Action:
      1. Create Premium connector (as necessary)
      2. Record SecCHM ID
      3. Move Environment to proper Data Policy (as needed)
2. User requests Prod Environment (Day 2)
   1. User Action:
      1. Create IR Works Request
   2. PPT Action:

# Review request – speak with User – Create Environment (see How to Add a Sandbox Environment

## Summary of Steps:

* Create Security groups
* Create Environment
  + Define environment Settings
* Create Environment Teams
* Notify User of environment creation

## Step 1: Create User Security Group

Reference: Power Platform Basics

To implement proper Power Platform application and flow development, the PPT will provide three environments as follows:

* Sandbox (Type: sandbox, unmanaged)
* Test (Type: production, managed)
* Production (Type: production, managed)

# Security for Power Platform Environments

The Power Platform Team does not provide individual access to Environments. PPT will use Microsoft Entra Security Groups to apply a role-based method for applying access to Power Platform Environments. This provides the user base with self-governance of access, while also providing Microsoft best-practice security for environments.

## Security Group Allocation

How to Create Security Groups for Power Platform

There should be a minimum of 3 groups created for a Sandbox or Development environment (this may vary based on needs and requests over time, especially when using Dataverse):

* Maker Group
  + Owners: Supplied via request (csv file) by the environment requestors.
  + Members: Supplied via request (csv file) by the environment requestors.
* Admin Group
  + Owners: PPT Team and Environment owning (IS THIS CORRECT – DO WE GIVE SYS ADMIN TO CLIENT?)
  + Members: None
* User Group
  + Owners: Supplied via request (csv file) by the environment requestors.
  + Members: Supplied via request (csv file) by the environment requestors.

## Step 2: Create Environment

1. Login into Power Platform Admin Center: https://gcc.admin.powerplatform.microsoft.us/?l=en-US
2. In the Power Platform admin center, click Environments on the left nav/tool bar

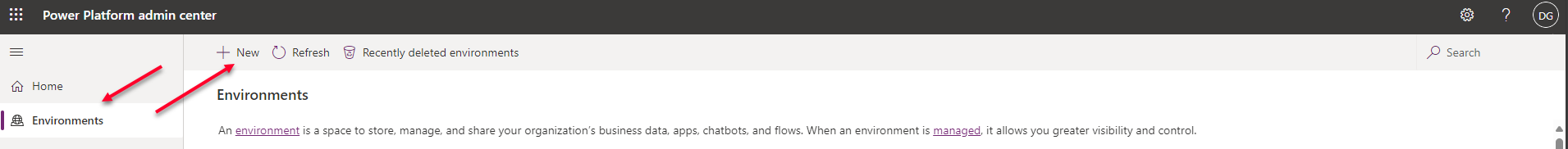


Figure 8

1. Click *New* to create a new environment (a New environment form comes up on the right side of the page)
2. Fields are filled out as follows:
   * New environment form:
     + **Name**: *[BU]-[APP]-Sandbox or [BU]-[APP]-Development*
       - Example: IT-EOPS-SPO-Sandbox / IT-EOPS-SPO-Development
     + **Region**: *GCC Default*
     + **Type**: *Sandbox (or Development)*
     + **Purpose**:
     + **Add a Dataverse data store?**: *Yes*
     + Click the *Next* button (which will bring up the Add Dataverse form)
   * Add Dataverse form:
     + **Language**: *English (United States)*
     + **Currency**: *USD ($)*
     + **Security group** (click + Select): *None*
     + **URL** (click here): *[bu]-[app]-sandbox (or [bu]-[app]-development)*
       - Example: it-eops-spo-sandbox or it-eops-spo-development
     + **Enable Dynamics 365 apps?**: *No*
     + **Deploy sample apps and data?**: *No*

|  |  |
| --- | --- |
| Figure 10 | Figure 11 |

## Step 3: Settings

Once you have created the environment, open the environment

1. If you are not already in, login into Power Platform Admin Center: https://gcc.admin.powerplatform.microsoft.us/?l=en-US
2. In the Power Platform admin center use the *Search* or browse to find the Power Platform environment you just created in Step 2.

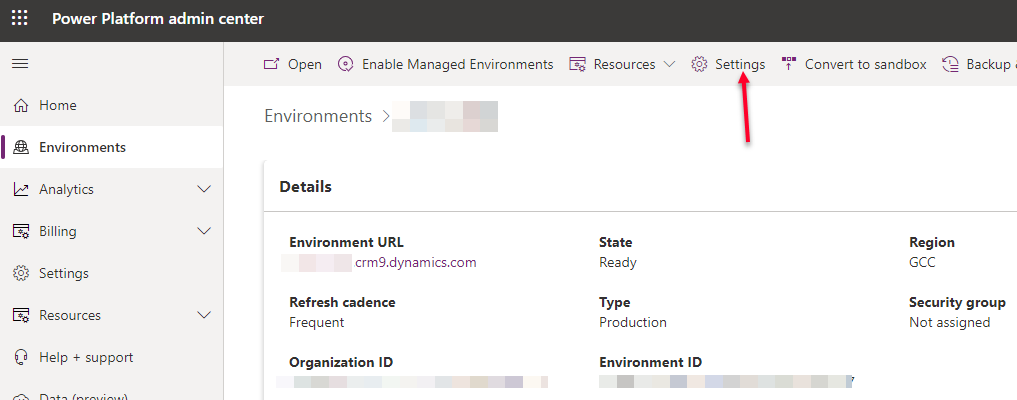


Figure 12

1. In the Details screen, in the upper tool bar, click on *Settings* to open up the Settings panel.

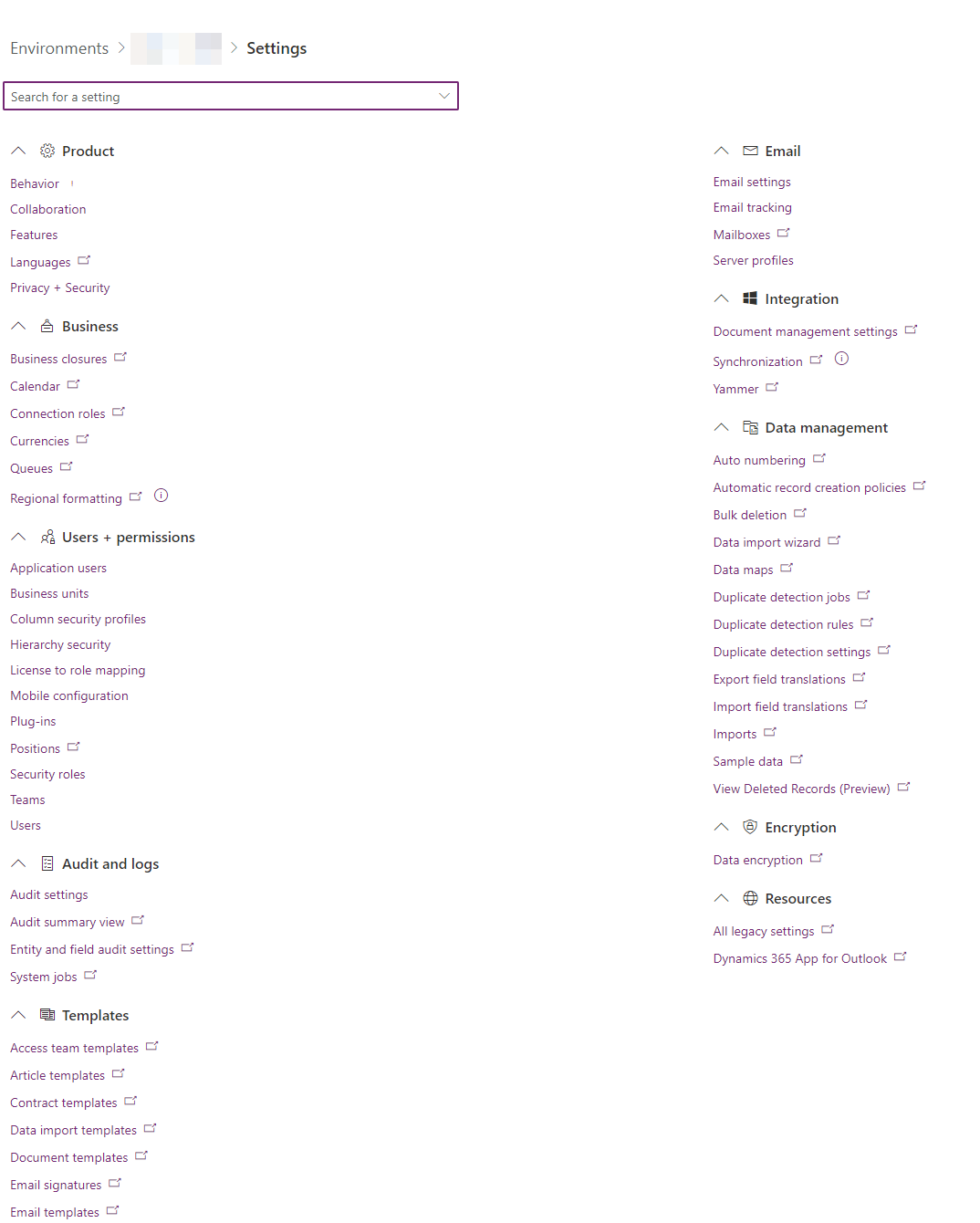


Figure 13

* 1. Under *Product* >
     1. *Behavior*
        1. Make no changes – accept all default settings.
     2. *Collaboration*
        1. Make no changes – accept all default settings.
     3. *Features*
        1. Make all changes as found in Figure #. Of note:
           1. **Allow canvas editors to insert the Copilot answer component, which allows users to receive an AI-powered answer to a predefined data query:** *Turn Off (see figure #: A)*
           2. AI Builder:

**Enable the usage of AI Builder model types that are in preview***: Turn Off* *(see figure #: A)*

* + - * 1. AI Prompts:

**Enable the AI prompts feature in Power Platform and Copilot Studio:** *Turn Off (see figure #: A)*

* + - * 1. Natural language grid and view search

**Find your data in model-driven app views with the help of Copilot.**

*No one*

* + - * 1. AI insight cards:

**Record summaries and other Copilot insights will appear on main forms**

*Turn Off*

* + - * 1. Power Automate Process Mining:

**Enable production ready preview features for Power Automate Process Mining.**

*Turn Off*

* + - * 1. Embedded Content:

**Power BI**: *Turn on* *(see figure #: B)*

* + - * 1. Hosted RPA:

**Enable hosted machine groups**: *Turn Off* *(see figure #: C)*

**Enable work or school accounts for hosted machine groups**: *Turn Off* *(see figure #: C)*

* + - * 1. Search

**Dataverse search**: *Turn On* *(see figure #: D)*

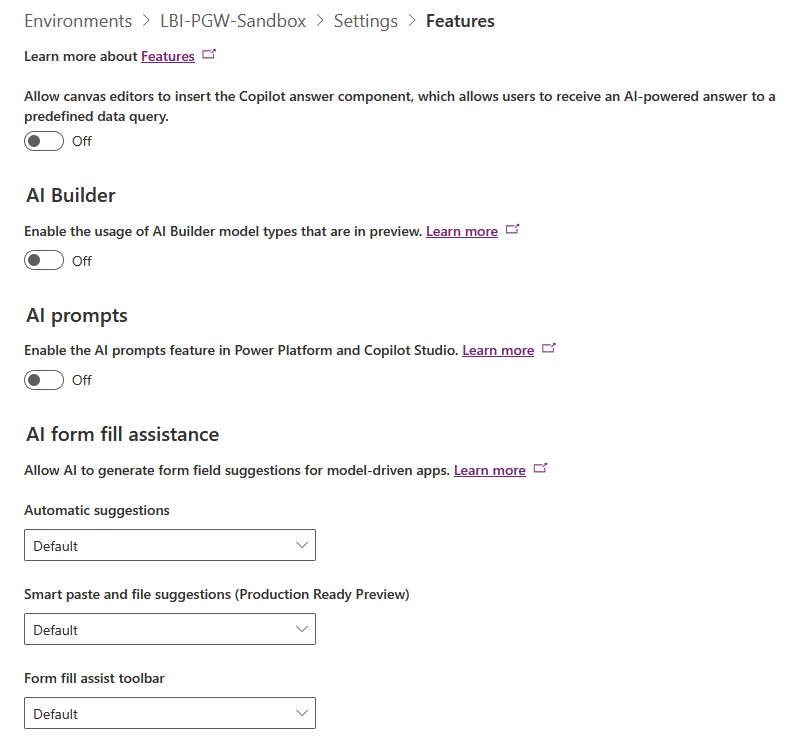
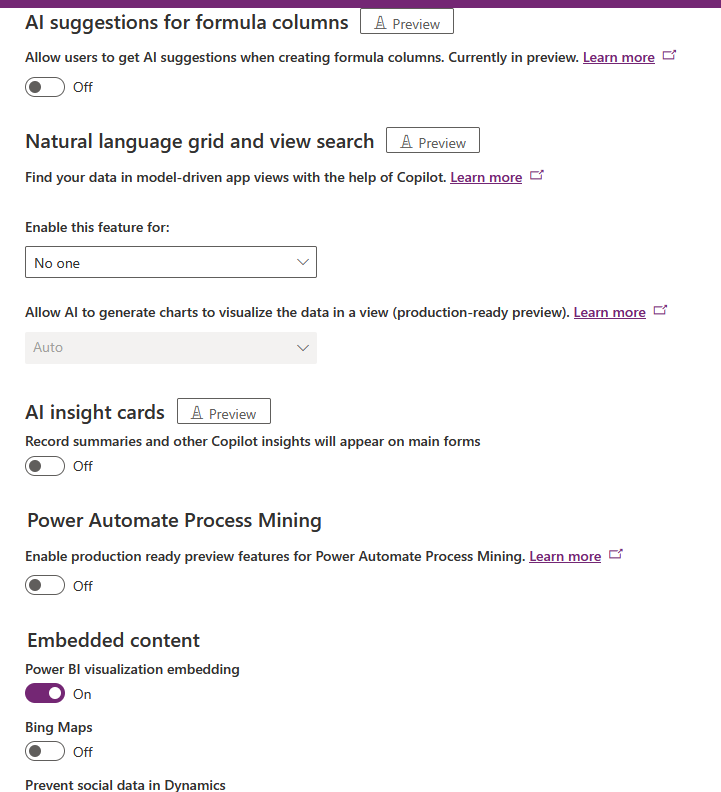
**Single Table Search Option**: *Turn On* *(see figure #: D)*

* + - * 1. Delete disabled users

**Enable delete disabled users**: *Turn On* *(see figure #: E)*

* + 1. *Privacy + Security*
       1. Privacy Preference
          1. **Show privacy statement link for this organization**: *Turn On* *(see figure #: A)*
          2. **Privacy statement URL**: *https://www.irs.gov/privacy-disclosure/irs-privacy-policy* *(see figure #: B)*
          3. **Default action to take when an error occurs**:

Choose > *Never send an error report to Microsoft* *(see figure #: C)*

** **

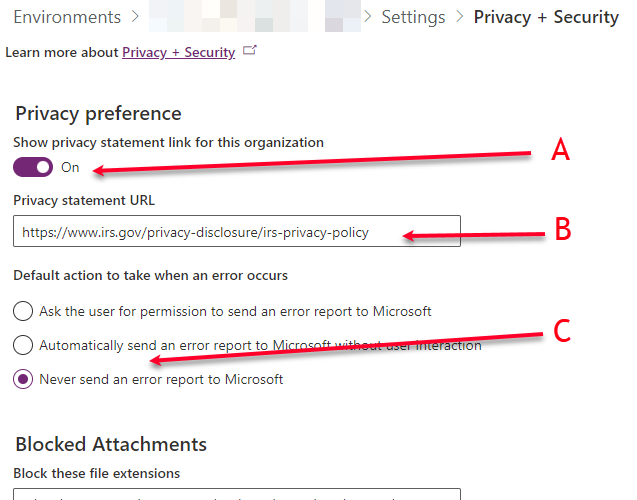


Figure 14

* 1. Under *Audit and Logs* >
     1. *Auditing*
        1. **Start Auditing**: *check on* *(see figure #: A)*
        2. **Log Access**: *check on* *(see figure #: A)*
        3. **Read Logs**: *check on* *(see figure #: A)*

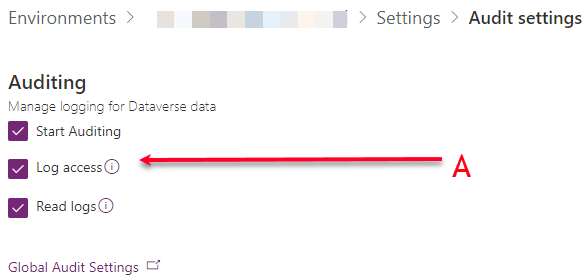


Figure 15

* + - 1. **Retain these logs for:** 2 Years = 730 Days
         1. \*\* NOTE \*\* You will need to wait up to 24 hours after creating the Environment for this Field to become available, so you will need to ensure you go back in the next day to set this field!
         2. Once you have waited long enough, go back into this section and you will now see this field (Figure 24).

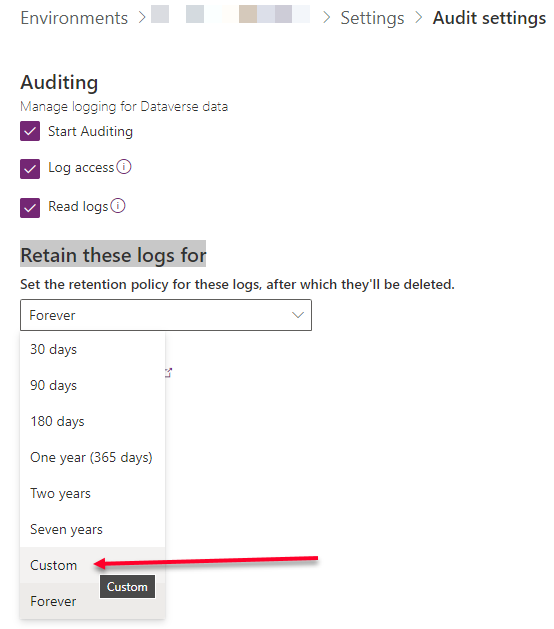


Figure 16

* + - * 1. From the drop-down, select Custom, and enter 1825 (days)

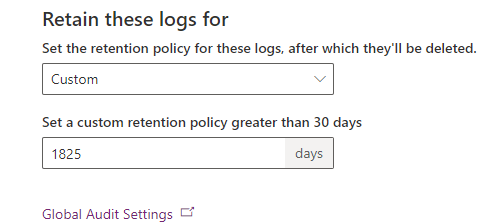


Figure 17

* 1. Under *Users + Permissions* >
     1. Teams
        1. Create team  
           This first team is the Power Platform Team Admins.
           1. **Team Name:** PP Tenant Admins
           2. **Description:** Power Platform role group covering tenant wide Power Platform admins (used to assign admin rights over all environments for IT support)
           3. **Business unit:** <bu name>-<app>-prod (all lowercase)

Example: sbse-transmittal-sandbox

* + - * 1. **Administrator:** <yourself as PP Admin> (currently your boad account)
        2. **Team type:** Microsoft Entra ID Security Group
        3. **Group name:** CLOUD USER M365 MPP IT EOPS PP ADMINS
        4. **Membership type:** Owners
        5. **Role:** System Administrator
      1. Create team (VERIFY THIS TEAM)
         1. **Team Name:** CLOUD M365 MPP <BU> DEV <APP NAME> ADMIN  
            Should be the same name as defined in *Step 1: Create User Security Group*

Example: CLOUD M365 MPP DEV [BU] [SOL] ADMIN

* + - * 1. **Description:** Admins in the <BU> <APP> Sandbox environment
        2. **Business unit:** <bu name>-<app>-prod (all lowercase)  
           Should be the same as the URL entered in the Dataverse Form when creating the Environment.

Example: [bu]-[app]-sandbox

* + - * 1. **Administrator:** <yourself as PP Admin> (currently your boad account)
        2. **Team type:** Microsoft Entra ID Security Group
        3. **Group name:** CLOUD M365 MPP DEV [BU] [SOL] ADMIN  
           Should be the same name as defined in *Step 1: Create User Security Group*
        4. **Membership type:** Members
        5. **Role:** System Administrator
      1. Create team
         1. **Team Name:** CLOUD M365 MPP <BU> DEV <APP NAME> MAKER  
            Should be the same name as defined in *Step 1: Create User Security Group*

Example: CLOUD M365 MPP DEV [BU] [SOL] MAKER

* + - * 1. **Description:** Makers in the <BU> <APP> Sandbox environment
        2. **Business unit:** <bu name>-<app>-prod (all lowercase)  
           Should be the same as the URL entered in the Dataverse Form when creating the Environment.

Example: [bu]-[app]-sandbox

* + - * 1. **Administrator:** <yourself as PP Admin> (currently your boad account)
        2. **Team type:** Microsoft Entra ID Security Group
        3. **Group name:** CLOUD M365 MPP DEV [BU] [SOL] MAKER  
           Should be the same name as defined in *Step 1: Create User Security Group*
        4. **Membership type:** Members
        5. **Role:** Environment maker and System customizer
      1. Create team
         1. **Team Name:** CLOUD M365 MPP <BU> DEV <APP NAME> USER  
            Should be the same name as defined in *Step 1: Create User Security Group*

Example: CLOUD M365 MPP DEV [BU] [SOL] USER

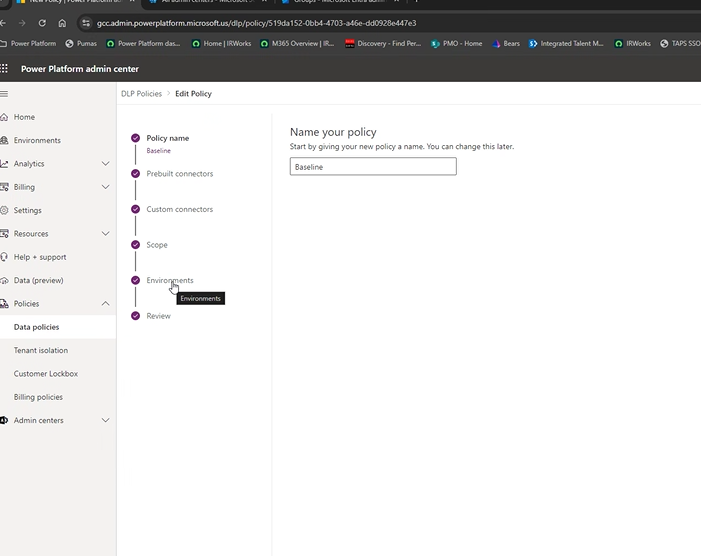
* + - * 1. **Description:** Users in the <BU> <APP> Sandbox environment
        2. **Business unit:** <bu name>-<app>-prod (all lowercase)  
           Should be the same as the URL entered in the Dataverse Form when creating the Environment.

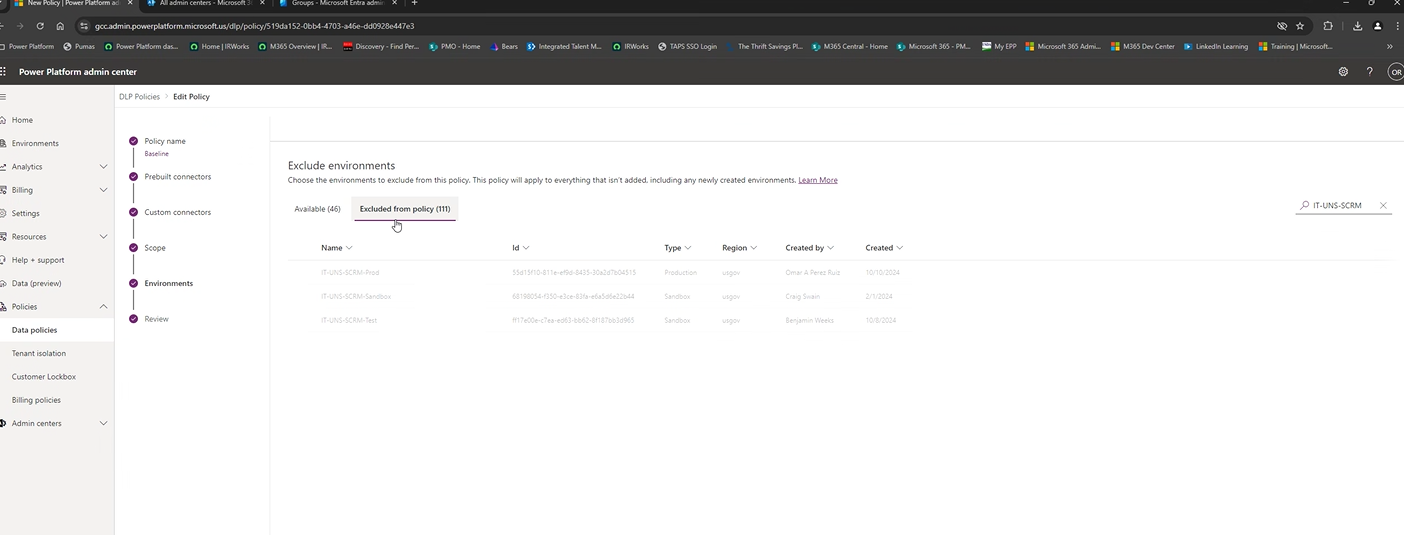
Example: [bu]-[app]-sandbox

* + - * 1. **Administrator:** <yourself as PP Admin> (currently your boad account)
        2. **Team type:** Microsoft Entra ID Security Group
        3. **Group name:** CLOUD M365 MPP DEV [BU] [SOL] USER  
           Should be the same name as defined in *Step 1: Create User Security Group*
        4. **Membership type:** Members
        5. **Role:** Basic user AND App Opener

## Step 4: Add to Proper Policy

1. Open Power Platform Admin Center
   * Policies > Data Policies
   * Add non-Dataverse environments to: Baseline
   * Add Dataverse environments to: Default Plus Dataverse
   * Add SQL approved environments to: SQL plus Dataverse
   * Add Oracle plus Dataverse to: Oracle plus Dataverse





## Step 5: Create Approval Tables

This is only necessary for those environments using Approval Microsoft built-in Approvals

1. SAM CAN ENTER THE STEPS Import and run flow to create Approvals Tables
   * 1. )
2. User requests one or more Security groups for their environment (Day 2)
   1. User Actions:
      1. Create IR Works Request for EACH group (include CVS for users)
         1. User Group
   2. PPT Action:
      1. Create the groups in Entra and then in the Sandbox (Development) environment.
         1. Review request
         2. speak with User

# Create each group (see Power Platform Basics

To implement proper Power Platform application and flow development, the PPT will provide three environments as follows:

* Sandbox (Type: sandbox, unmanaged)
* Test (Type: production, managed)
* Production (Type: production, managed)

# Security for Power Platform Environments

The Power Platform Team does not provide individual access to Environments. PPT will use Microsoft Entra Security Groups to apply a role-based method for applying access to Power Platform Environments. This provides the user base with self-governance of access, while also providing Microsoft best-practice security for environments.

## Security Group Allocation

* + - 1. How to Create Security Groups for Power Platform)

1. User requests premium connectors for Prod (Day 2)
   1. User Action:
      1. Create Change Request for Premium Connection
      2. Obtain SecCHM ID
      3. Provide that to us for documentation.
2. PPT Action:
   * 1. Create Premium connector (as necessary)
     2. Record SecCHM ID
     3. Move Environment to proper Data Policy (as needed)
3. User requests Solution Deployment (Day 3 - 7)
   1. User Action:
      1. Submit Request
      2. Include Solution Architecture
   2. PPT Action:
      1. Review Solution
      2. Approve / Deny solution
         1. Approve – Deploy Solution
         2. Denied – Give feedback and await updates to Architecture and cycle through this effort until approved or cancelled.
4. Pipelines
   1. If Steps 1 – 6 are complete and user would like to set up a Pipeline:
      1. Ensure that Architecture has been approved before providing deployment capability.
         1. Limit deployment by Solution (**CAN WE DO THIS ????**)

**\*\* UPDATES REQUIRED**

1. If User has already deployed to production but requests:
   1. A new Premium Connector
   2. A new Security group
2. Require a change to their Architecture before performing.

# Power Platform Basics

To implement proper Power Platform application and flow development, the PPT will provide three environments as follows:

* Sandbox (Type: sandbox, unmanaged)
* Test (Type: production, managed)
* Production (Type: production, managed)

# Security for Power Platform Environments

The Power Platform Team does not provide individual access to Environments. PPT will use Microsoft Entra Security Groups to apply a role-based method for applying access to Power Platform Environments. This provides the user base with self-governance of access, while also providing Microsoft best-practice security for environments.

## Security Group Allocation

# How to Create Security Groups for Power Platform

There are two steps for creating a Security group for a Power Platform environment:

* Create a Microsoft Entra Security Group  
  The owners of these groups have the rights and privileges to add/remove members to these groups – which takes the responsibility out of the PPT’s hands and allows them to self maintain.
* Create a Team in the Power Platform Environment and attach the Microsoft Entra Security Group to a Team within the Power Platform Environment.

It is recommended that all Security Groups should be specific to the environment (i.e. Sandbox, Development, Test, or Prod). This is primarily to ensure the prevention of conflict between environments.

## Security Group Naming Conventions

Our naming convention is as follows (ALL CAPS):

CLOUD M365 MPP [ENV] [BU] [SOL] [USER TYPE]

* [ENV] = Environment (i.e. Sandbox or Development (DEV), Test (TST), Production (PROD))
* [BU] = Business Unit (i.e. IT-EOPS, PGLD, TS, SBSE, etc.)
* [SOL] = Solution (the core Solution that the environment will hold) or if this is a multi-solution environment, you may use the BU again here, otherwise it should be the Solution name or abbreviation.
* [USER TYPE] = the type of user the group will hold (i.e. basic users (USER), Makers (MAKER), Admins (ADMIN))
  + \*\* NOTE that you may have other names specific their role for environments that have Dataverse and different users based on their Dataverse access.

Each Environment should have the minimum Groups:

* Sandbox
  + Maker Group : CLOUD M365 MPP DEV [BU] [SOL] MAKER
  + User Group : CLOUD M365 MPP DEV [BU] [SOL] USER
* Development
  + Maker Group : CLOUD M365 MPP DEV [BU] [SOL] MAKER
  + User Group: CLOUD M365 MPP DEV [BU] [SOL] USER
* Test
  + User Group : CLOUD M365 MPP TEST [BU] [SOL] USER
* Production
  + User Group : CLOUD M365 MPP PROD [BU] [SOL] USER

## Microsoft Entra Security groups

Using the above Naming Convention:

1. Login into Microsoft Entra: <https://entra.microsoft.com/>
2. On the left Tool bar select Identity à Groups à All groups (Figure 3).

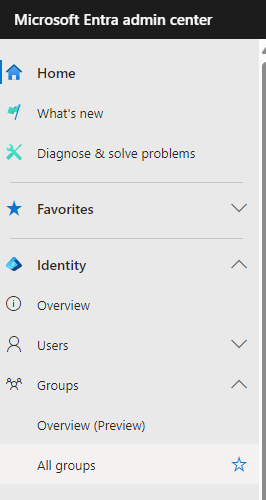


Figure 1

1. In the main pane, select New group

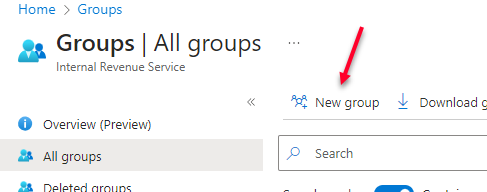


Figure 2

1. In the New group panel, fill in the fields as follows:
   1. Group type: Security
   2. Group Name: See Security Group Naming Conventions above.
   3. Group description:
   4. Membership type: Assigned

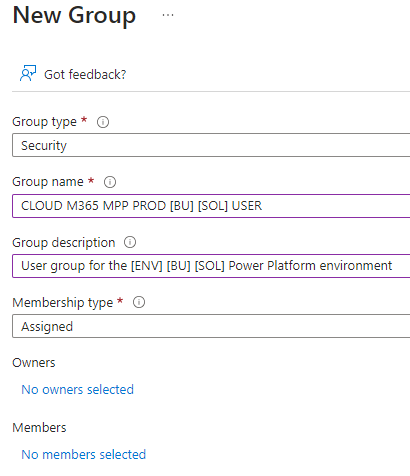
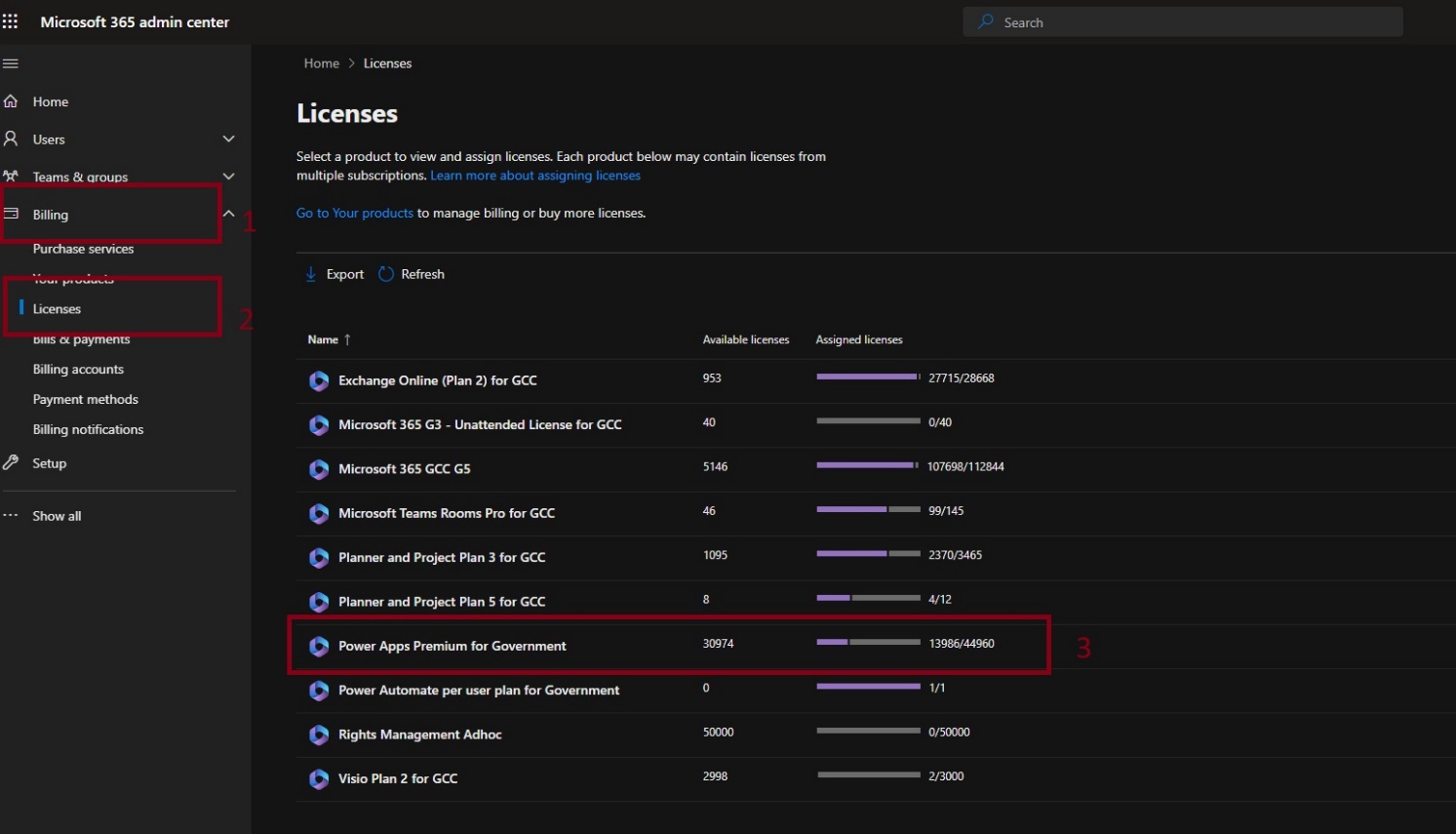
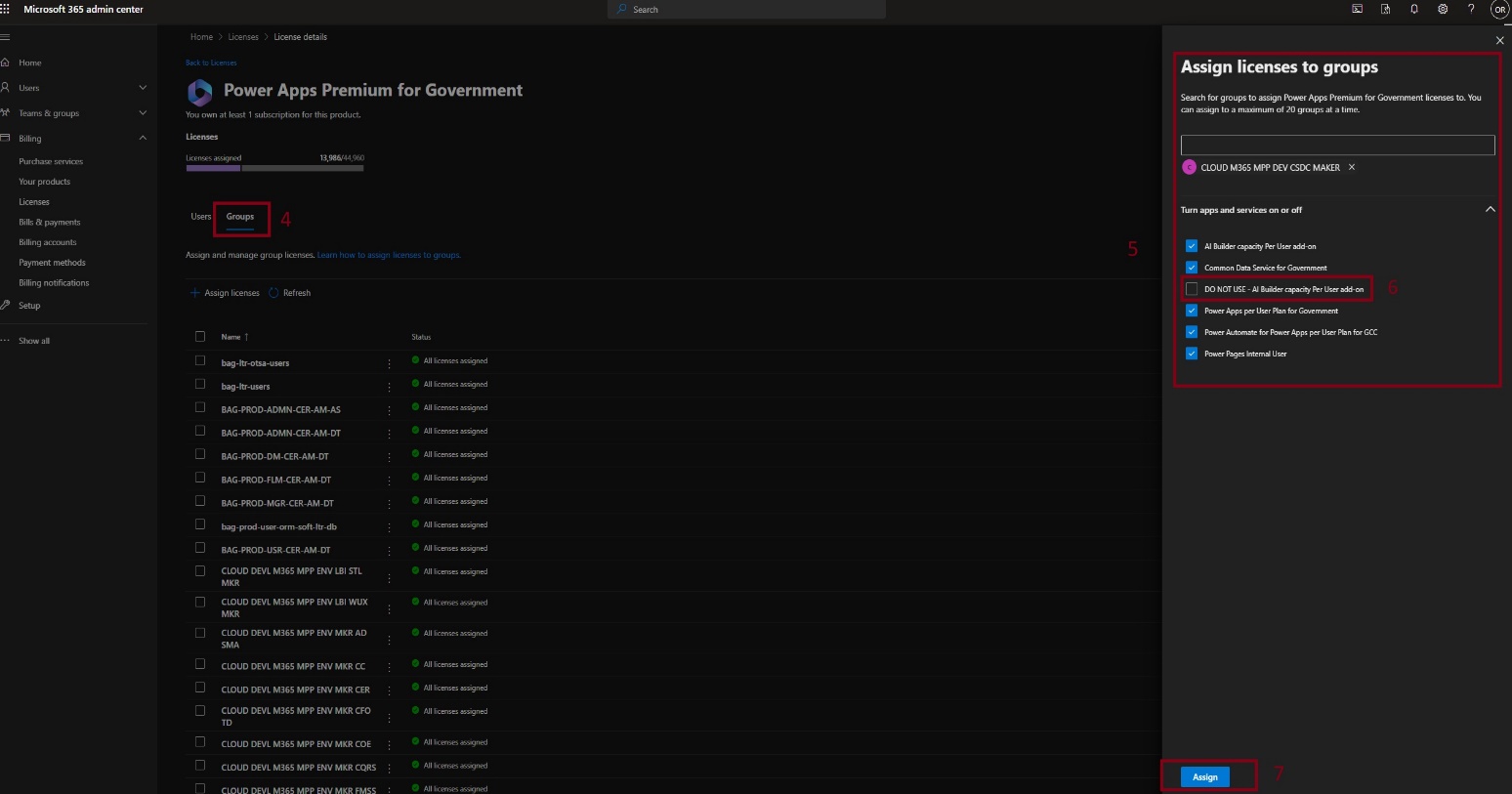
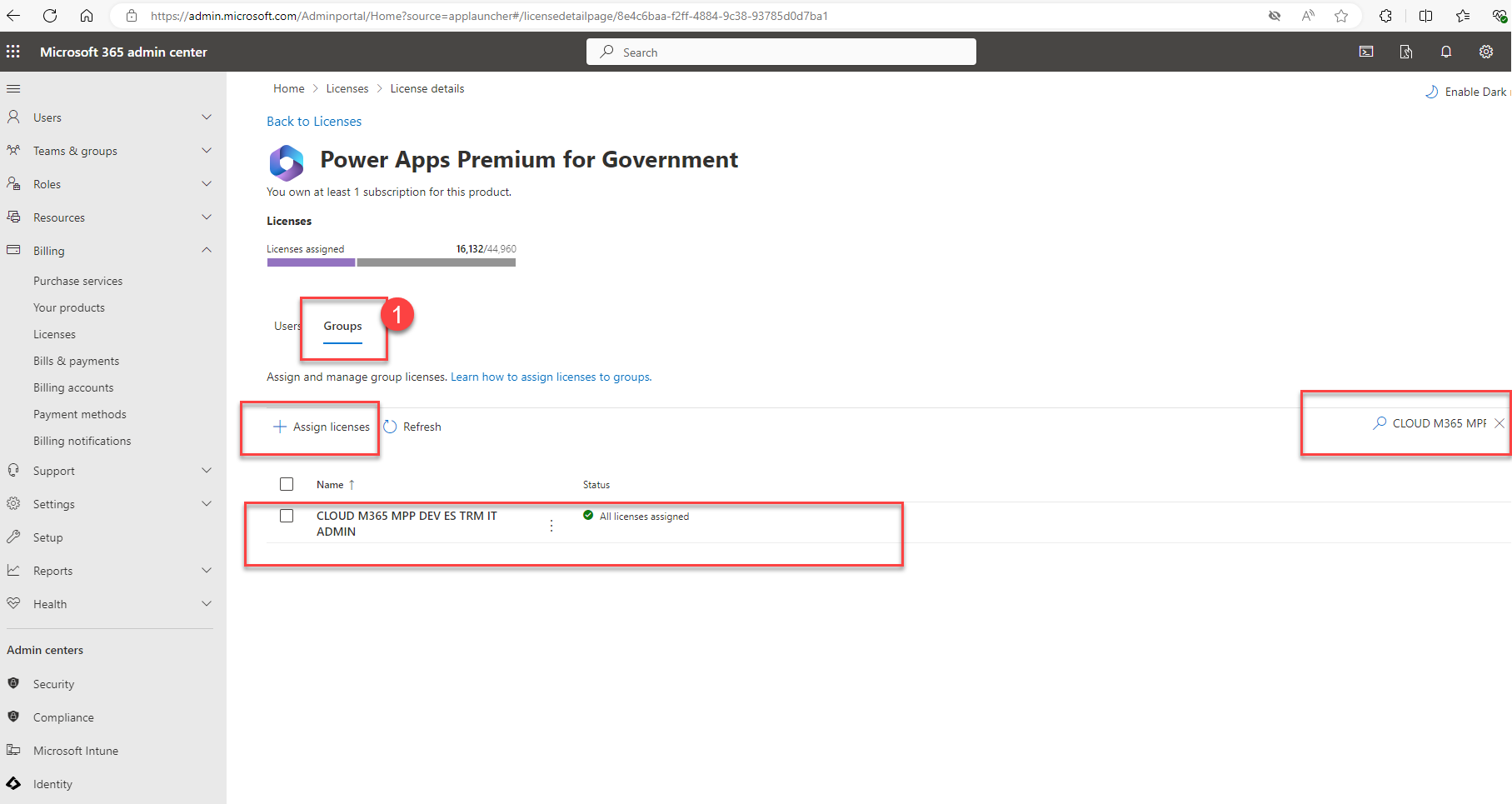


Figure 3

1. Add Owner as follows:
   1. Sandbox
      1. Maker Group : CLOUD M365 MPP DEV [BU] [SOL] MAKER
         1. BU Environment Owners
      2. User Group : CLOUD M365 MPP DEV [BU] [SOL] USER
         1. BU Environment Owners
   2. Development
      1. Maker Group : CLOUD M365 MPP DEV [BU] [SOL] MAKER
         1. BU Environment Owners
      2. User Group: CLOUD M365 MPP DEV [BU] [SOL] USER
         1. BU Environment Owners
   3. Test
      1. User Group : CLOUD M365 MPP TST [BU] [SOL] USER
         1. BU Environment Owners
   4. Production
      1. User Group : CLOUD M365 MPP PROD [BU] [SOL] USER
         1. BU Environment Owners
2. Add members as follows:
   1. For each group, the BU requestor should be providing a CVS list of users that may be individually added or may be bulk added.
3. Add the group to the Power Apps Premium for Government
   1. Go to <https://admin.microsoft.com/Adminportal/Home?#/homepage>
   2. Select Billing and then License.
   3. Select Power Apps Premium for Government
   4. Go to the Groups Tab and press +Assign licenses.
   5. Enter the Security Group name.
   6. Select Turn apps and services on or off and remove \*DO NOT USE – AI Builder capacity Per User add-on.
   7. Press Assign.







## Attaching the Entra Security Group to a Power Platform Team

Once you have created the Power Platform Environment (see How to Add a Sandbox Environment or **Error! Reference source not found.**) you need to create the appropriate Teams in the Power Platform environment and attach the appropriate Entra Security Group.

1. Log into the Power Platform admin center: <https://gcc.admin.powerplatform.microsoft.us/?l=en-US>
2. In the Power Platform admin center under Environments, click on the Search and find the Power Platform environment you created or need to modify user groups for.

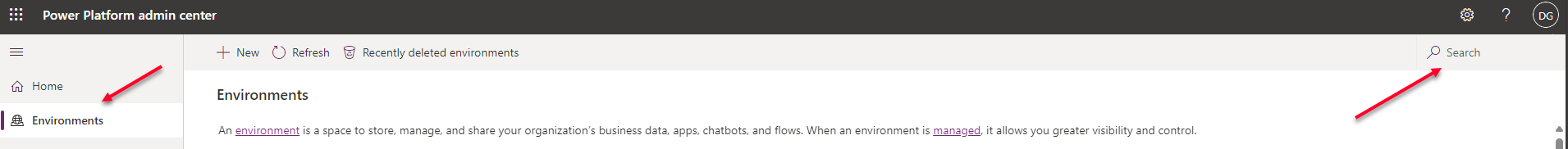


Figure 4

1. Once you have found the environment click on the environment name to open up the Environment Details

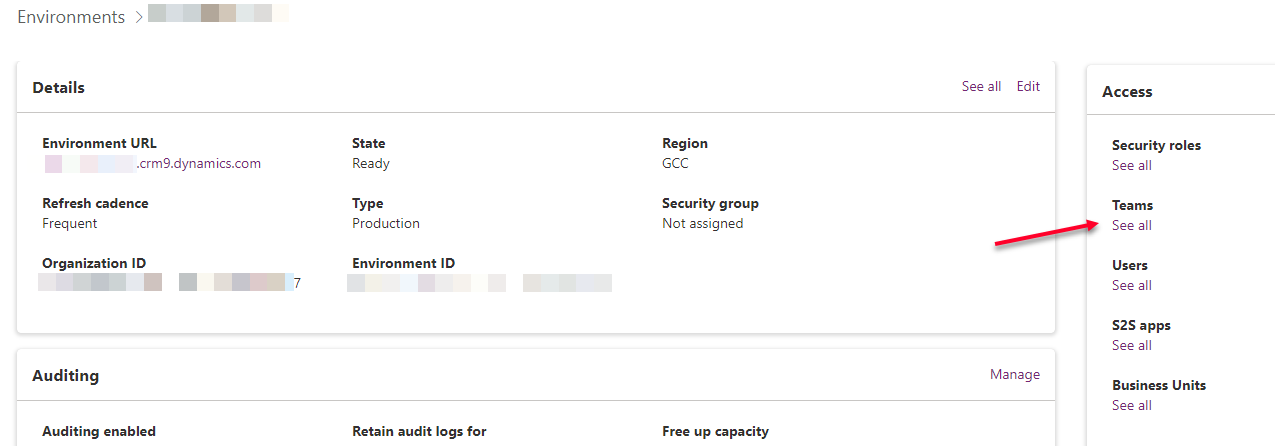


Figure 5

1. Under the Access pane, click on See all under Teams
2. In the Teams pane, click on Create team

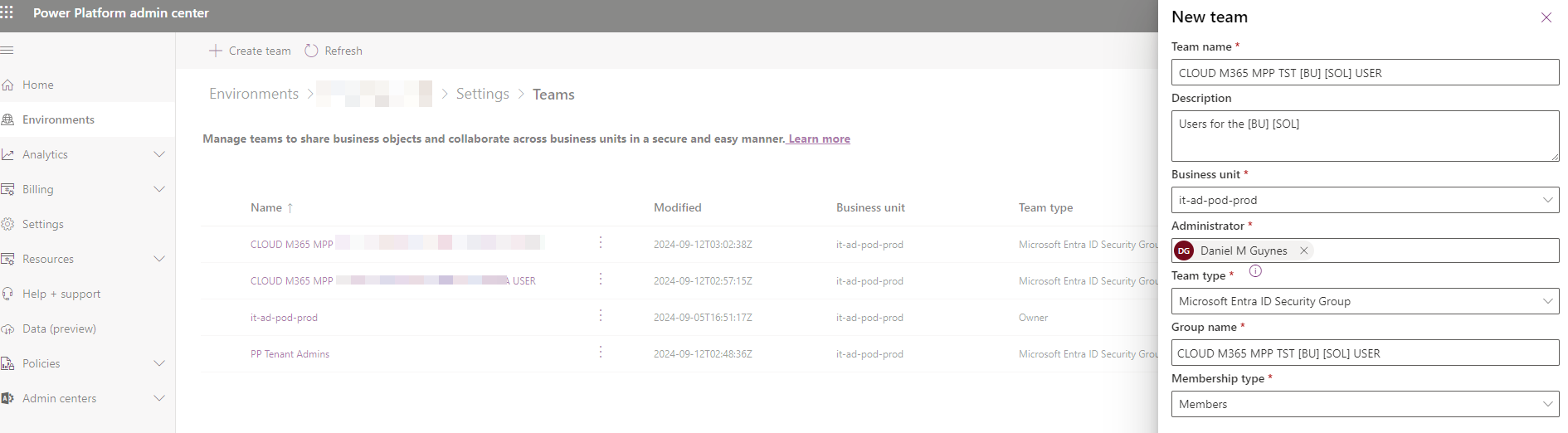


Figure 6

# Team name: should be the same as the Entra Security group you created (see Power Platform Basics

To implement proper Power Platform application and flow development, the PPT will provide three environments as follows:

* Sandbox (Type: sandbox, unmanaged)
* Test (Type: production, managed)
* Production (Type: production, managed)

# Security for Power Platform Environments

The Power Platform Team does not provide individual access to Environments. PPT will use Microsoft Entra Security Groups to apply a role-based method for applying access to Power Platform Environments. This provides the user base with self-governance of access, while also providing Microsoft best-practice security for environments.

## Security Group Allocation

* 1. How to Create Security Groups for Power Platform)
  2. Description:
  3. Business unit: should be the default business unit (it is possible to have multiple which is a more advanced topic)
  4. Administrator: Add you BOAD account (this may change later to be by a Group)
  5. Team type: Microsoft Entra ID Security Group

# Group name: Add the Entra Security group created in Power Platform Basics

To implement proper Power Platform application and flow development, the PPT will provide three environments as follows:

* Sandbox (Type: sandbox, unmanaged)
* Test (Type: production, managed)
* Production (Type: production, managed)

# Security for Power Platform Environments

The Power Platform Team does not provide individual access to Environments. PPT will use Microsoft Entra Security Groups to apply a role-based method for applying access to Power Platform Environments. This provides the user base with self-governance of access, while also providing Microsoft best-practice security for environments.

## Security Group Allocation

* 1. How to Create Security Groups for Power Platform.
  2. Membership type: Members

### Add Security Roles to the Teams

Once you have created the Power Platform environment Team and synchronized it with the Entra Security Group, you must provide it the proper Security role on the environment.

1. If you are automatically taken there after the creation of the Team continue to step 3, else,
2. Going back to the Teams page (see Figure )
   1. Click the three dots next to the Team you want to add a Security role to and select Manage security roles

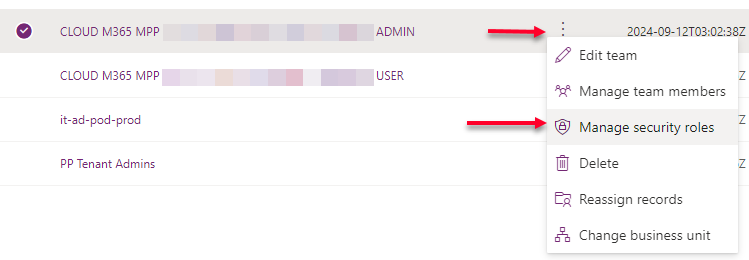


Figure 7

* 1. Add the appropriate Security role to the Team as follows:  
     \*\* NOTE \*\* ask one of us if the team or security role is outside of these defults
     1. Sandbox
        1. Maker Group : CLOUD M365 MPP DEV [BU] [SOL] MAKER
           1. Security role(s): Environment Maker, System Customizer
        2. User Group : CLOUD M365 MPP DEV [BU] [SOL] USER
           1. Security role(s): Basic User
     2. Development
        1. Maker Group : CLOUD M365 MPP DEV [BU] [SOL] MAKER
           1. Security role(s): Environment Maker, System Customizer
        2. User Group: CLOUD M365 MPP DEV [BU] [SOL] USER
           1. Security role(s): Basic User
     3. Test
        1. User Group : CLOUD M365 MPP TST [BU] [SOL] USER
           1. Security role(s): Basic User
     4. Production
        1. User Group : CLOUD M365 MPP PROD [BU] [SOL] USER
           1. Security role(s): Basic User \*make administrator be the creator of the env
  2. NOTE that there are exceptions to Dataverse security roles and requirements for groups needed that have specific rights related to Dataverse.

# How to Add a Sandbox Environment

## Summary of Steps:

* Create Security groups
* Create Environment
  + Define environment Settings
* Create Environment Teams
* Notify User of environment creation

## Step 1: Create User Security Group

Reference: Power Platform Basics

To implement proper Power Platform application and flow development, the PPT will provide three environments as follows:

* Sandbox (Type: sandbox, unmanaged)
* Test (Type: production, managed)
* Production (Type: production, managed)

# Security for Power Platform Environments

The Power Platform Team does not provide individual access to Environments. PPT will use Microsoft Entra Security Groups to apply a role-based method for applying access to Power Platform Environments. This provides the user base with self-governance of access, while also providing Microsoft best-practice security for environments.

## Security Group Allocation

How to Create Security Groups for Power Platform

There should be a minimum of 3 groups created for a Sandbox or Development environment (this may vary based on needs and requests over time, especially when using Dataverse):

* Maker Group
  + Owners: Supplied via request (csv file) by the environment requestors.
  + Members: Supplied via request (csv file) by the environment requestors.
* Admin Group
  + Owners: PPT Team and Environment owning (IS THIS CORRECT – DO WE GIVE SYS ADMIN TO CLIENT?)
  + Members: None
* User Group
  + Owners: Supplied via request (csv file) by the environment requestors.
  + Members: Supplied via request (csv file) by the environment requestors.

## Step 2: Create Environment

1. Login into Power Platform Admin Center: <https://gcc.admin.powerplatform.microsoft.us/?l=en-US>
2. In the Power Platform admin center, click Environments on the left nav/tool bar

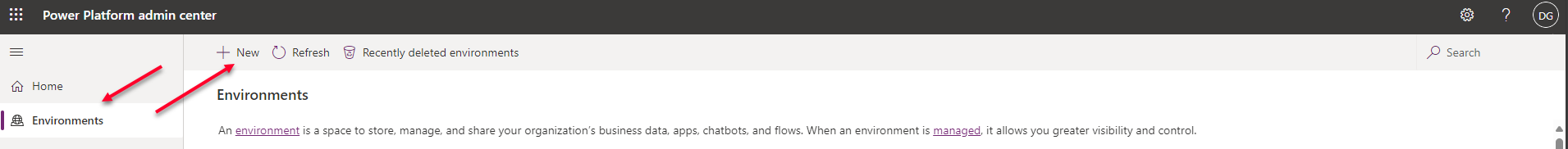


Figure 8

1. Click *New* to create a new environment (a New environment form comes up on the right side of the page)

Figure 9

1. Fields are filled out as follows:
   * New environment form:
     + **Name**: *[BU]-[APP]-Sandbox or [BU]-[APP]-Development*
       - Example: IT-EOPS-SPO-Sandbox / IT-EOPS-SPO-Development
     + **Region**: *GCC Default*
     + **Type**: *Sandbox (or Development)*
     + **Purpose**:
     + **Add a Dataverse data store?**: *Yes*
     + Click the *Next* button (which will bring up the Add Dataverse form)
   * Add Dataverse form:
     + **Language**: *English (United States)*
     + **Currency**: *USD ($)*
     + **Security group** (click + Select): *None*
     + **URL** (click here): *[bu]-[app]-sandbox (or [bu]-[app]-development)*
       - Example: it-eops-spo-sandbox or it-eops-spo-development
     + **Enable Dynamics 365 apps?**: *No*
     + **Deploy sample apps and data?**: *No*

|  |  |
| --- | --- |
| Figure 10 | Figure 11 |

## Step 3: Settings

Once you have created the environment, open the environment

1. If you are not already in, login into Power Platform Admin Center: <https://gcc.admin.powerplatform.microsoft.us/?l=en-US>
2. In the Power Platform admin center use the *Search* or browse to find the Power Platform environment you just created in Step 2.

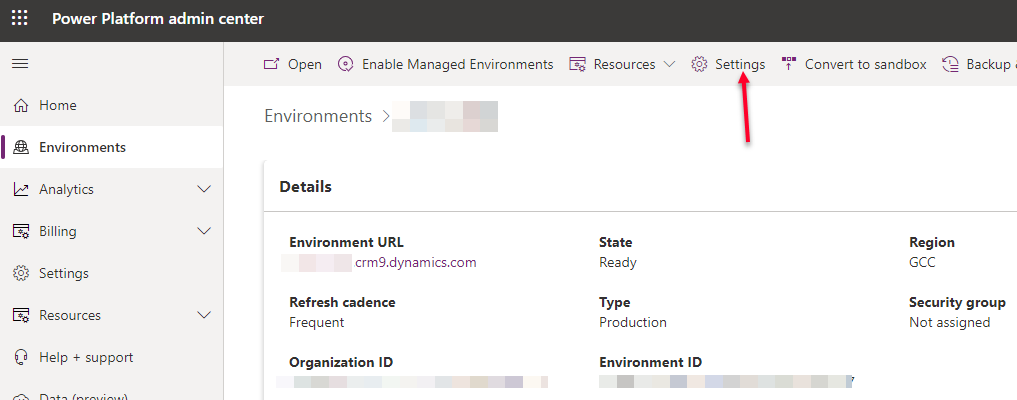


Figure 12

1. In the Details screen, in the upper tool bar, click on *Settings* to open up the Settings panel.

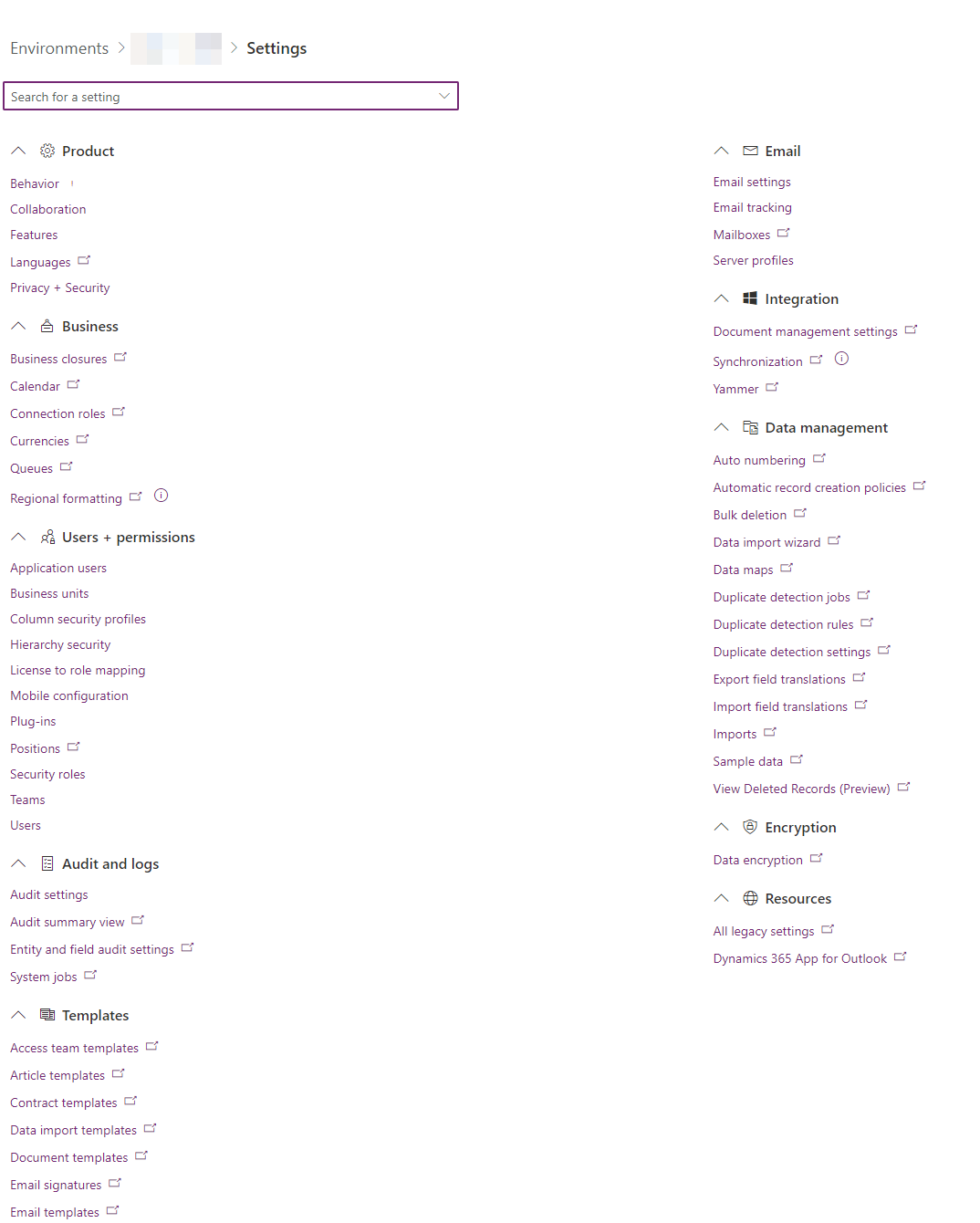


Figure 13

* 1. Under *Product* >
     1. *Behavior*
        1. Make no changes – accept all default settings.
     2. *Collaboration*
        1. Make no changes – accept all default settings.
     3. *Features*
        1. Make all changes as found in Figure #. Of note:
           1. **Allow canvas editors to insert the Copilot answer component, which allows users to receive an AI-powered answer to a predefined data query:** *Turn Off (see figure #: A)*
           2. AI Builder:

**Enable the usage of AI Builder model types that are in preview***: Turn Off* *(see figure #: A)*

* + - * 1. AI Prompts:

**Enable the AI prompts feature in Power Platform and Copilot Studio:** *Turn Off (see figure #: A)*

* + - * 1. Natural language grid and view search

**Find your data in model-driven app views with the help of Copilot.**

*No one*

* + - * 1. AI insight cards:

**Record summaries and other Copilot insights will appear on main forms**

*Turn Off*

* + - * 1. Power Automate Process Mining:

**Enable production ready preview features for Power Automate Process Mining.**

*Turn Off*

* + - * 1. Embedded Content:

**Power BI**: *Turn on* *(see figure #: B)*

* + - * 1. Hosted RPA:

**Enable hosted machine groups**: *Turn Off* *(see figure #: C)*

**Enable work or school accounts for hosted machine groups**: *Turn Off* *(see figure #: C)*

* + - * 1. Search

**Dataverse search**: *Turn On* *(see figure #: D)*

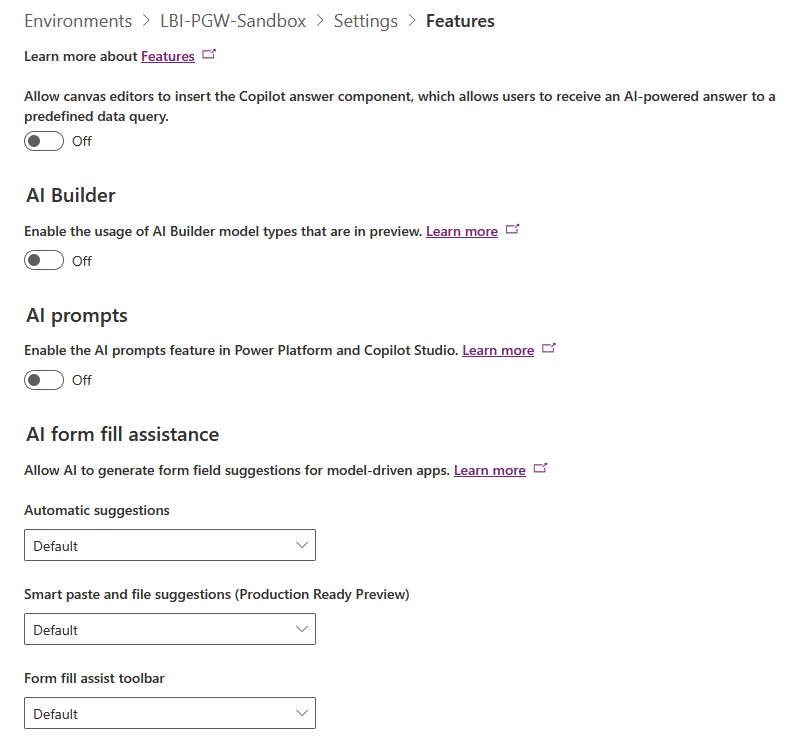
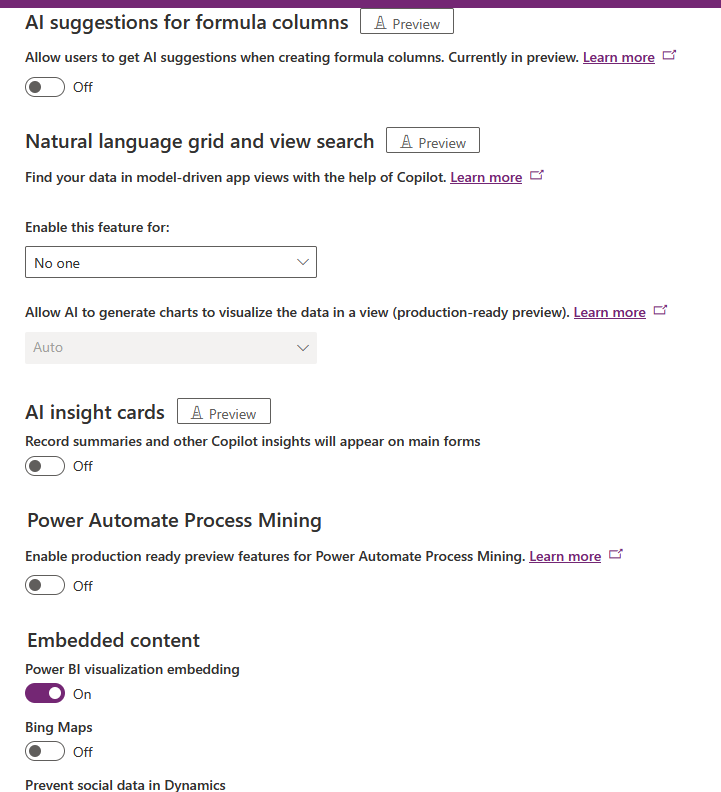
**Single Table Search Option**: *Turn On* *(see figure #: D)*

* + - * 1. Delete disabled users

**Enable delete disabled users**: *Turn On* *(see figure #: E)*

* + 1. *Privacy + Security*
       1. Privacy Preference
          1. **Show privacy statement link for this organization**: *Turn On* *(see figure #: A)*
          2. **Privacy statement URL**:[*https://www.irs.gov/privacy-disclosure/irs-privacy-policy*](https://www.irs.gov/privacy-disclosure/irs-privacy-policy) *(see figure #: B)*
          3. **Default action to take when an error occurs**:

Choose > *Never send an error report to Microsoft* *(see figure #: C)*

** **

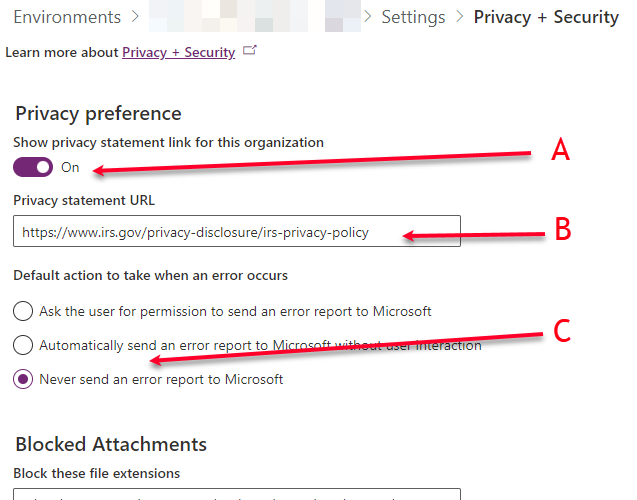


Figure 14

* 1. Under *Audit and Logs* >
     1. *Auditing*
        1. **Start Auditing**: *check on* *(see figure #: A)*
        2. **Log Access**: *check on* *(see figure #: A)*
        3. **Read Logs**: *check on* *(see figure #: A)*

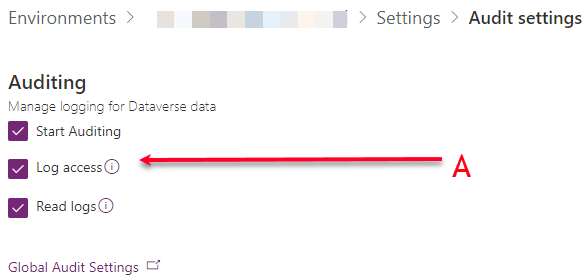


Figure 15

* + - 1. **Retain these logs for:** 2 Years = 730 Days
         1. \*\* NOTE \*\* You will need to wait up to 24 hours after creating the Environment for this Field to become available, so you will need to ensure you go back in the next day to set this field!
         2. Once you have waited long enough, go back into this section and you will now see this field (Figure 24).

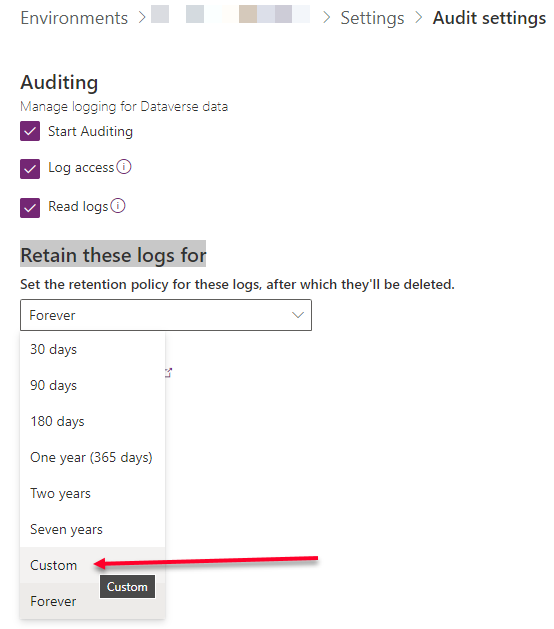


Figure 16

* + - * 1. From the drop-down, select Custom, and enter 1825 (days)

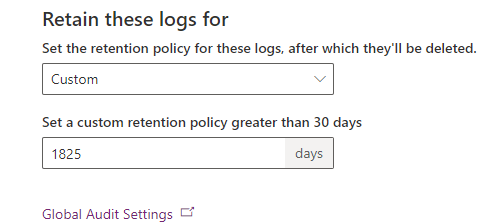


Figure 17

* 1. Under *Users + Permissions* >
     1. Teams
        1. Create team  
           This first team is the Power Platform Team Admins.
           1. **Team Name:** PP Tenant Admins
           2. **Description:** Power Platform role group covering tenant wide Power Platform admins (used to assign admin rights over all environments for IT support)
           3. **Business unit:** <bu name>-<app>-prod (all lowercase)

Example: sbse-transmittal-sandbox

* + - * 1. **Administrator:** <yourself as PP Admin> (currently your boad account)
        2. **Team type:** Microsoft Entra ID Security Group
        3. **Group name:** CLOUD USER M365 MPP IT EOPS PP ADMINS
        4. **Membership type:** Owners
        5. **Role:** System Administrator
      1. Create team (VERIFY THIS TEAM)
         1. **Team Name:** CLOUD M365 MPP <BU> DEV <APP NAME> ADMIN  
            Should be the same name as defined in *Step 1: Create User Security Group*

Example: CLOUD M365 MPP DEV [BU] [SOL] ADMIN

* + - * 1. **Description:** Admins in the <BU> <APP> Sandbox environment
        2. **Business unit:** <bu name>-<app>-prod (all lowercase)  
           Should be the same as the URL entered in the Dataverse Form when creating the Environment.

Example: [bu]-[app]-sandbox

* + - * 1. **Administrator:** <yourself as PP Admin> (currently your boad account)
        2. **Team type:** Microsoft Entra ID Security Group
        3. **Group name:** CLOUD M365 MPP DEV [BU] [SOL] ADMIN  
           Should be the same name as defined in *Step 1: Create User Security Group*
        4. **Membership type:** Members
        5. **Role:** System Administrator
      1. Create team
         1. **Team Name:** CLOUD M365 MPP <BU> DEV <APP NAME> MAKER  
            Should be the same name as defined in *Step 1: Create User Security Group*

Example: CLOUD M365 MPP DEV [BU] [SOL] MAKER

* + - * 1. **Description:** Makers in the <BU> <APP> Sandbox environment
        2. **Business unit:** <bu name>-<app>-prod (all lowercase)  
           Should be the same as the URL entered in the Dataverse Form when creating the Environment.

Example: [bu]-[app]-sandbox

* + - * 1. **Administrator:** <yourself as PP Admin> (currently your boad account)
        2. **Team type:** Microsoft Entra ID Security Group
        3. **Group name:** CLOUD M365 MPP DEV [BU] [SOL] MAKER  
           Should be the same name as defined in *Step 1: Create User Security Group*
        4. **Membership type:** Members
        5. **Role:** Environment maker and System customizer
      1. Create team
         1. **Team Name:** CLOUD M365 MPP <BU> DEV <APP NAME> USER  
            Should be the same name as defined in *Step 1: Create User Security Group*

Example: CLOUD M365 MPP DEV [BU] [SOL] USER

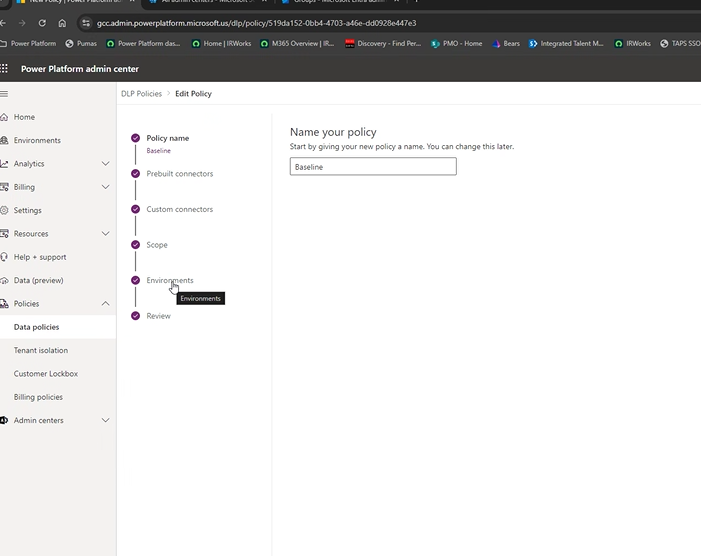
* + - * 1. **Description:** Users in the <BU> <APP> Sandbox environment
        2. **Business unit:** <bu name>-<app>-prod (all lowercase)  
           Should be the same as the URL entered in the Dataverse Form when creating the Environment.

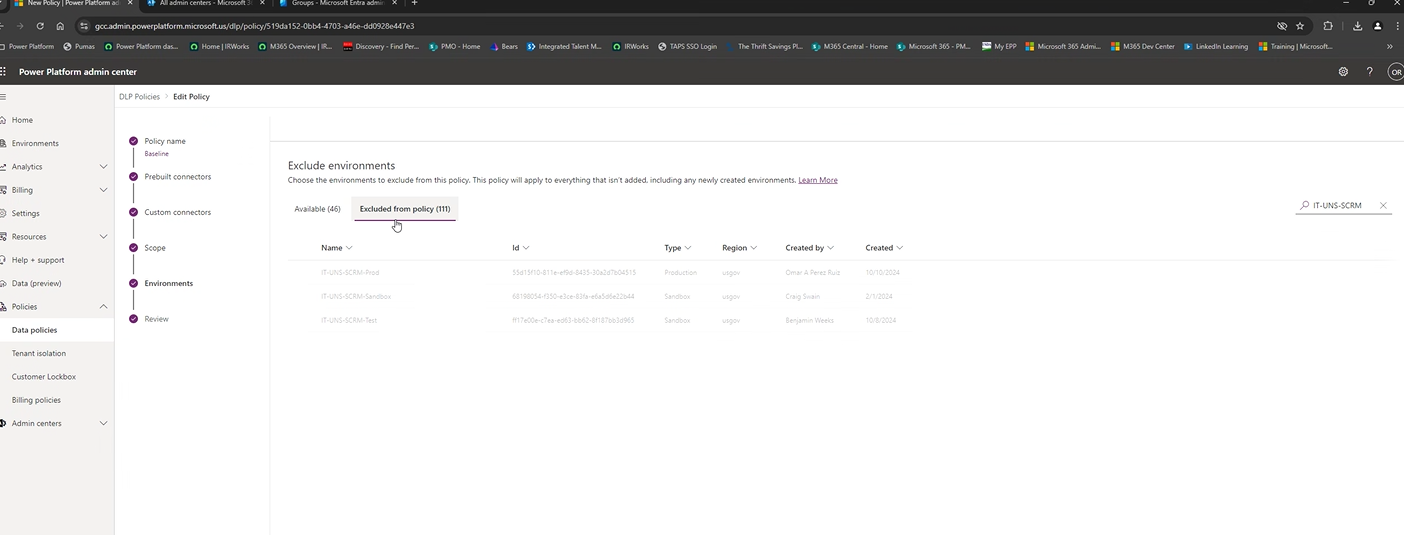
Example: [bu]-[app]-sandbox

* + - * 1. **Administrator:** <yourself as PP Admin> (currently your boad account)
        2. **Team type:** Microsoft Entra ID Security Group
        3. **Group name:** CLOUD M365 MPP DEV [BU] [SOL] USER  
           Should be the same name as defined in *Step 1: Create User Security Group*
        4. **Membership type:** Members
        5. **Role:** Basic user AND App Opener

## Step 4: Add to Proper Policy

1. Open Power Platform Admin Center
   * Policies > Data Policies
   * Add non-Dataverse environments to: Baseline
   * Add Dataverse environments to: Default Plus Dataverse
   * Add SQL approved environments to: SQL plus Dataverse
   * Add Oracle plus Dataverse to: Oracle plus Dataverse





## Step 5: Create Approval Tables

This is only necessary for those environments using Approval Microsoft built-in Approvals

1. SAM CAN ENTER THE STEPS Import and run flow to create Approvals Tables

# How to Add a Production And Test Environment

## Summary of Steps:

* Create Security groups
* Create Environment
  + Define environment Settings
* Create Environment Teams
* Notify User of environment creation

## Step 1: Create User Security Group

Reference: Power Platform Basics

To implement proper Power Platform application and flow development, the PPT will provide three environments as follows:

* Sandbox (Type: sandbox, unmanaged)
* Test (Type: production, managed)
* Production (Type: production, managed)

# Security for Power Platform Environments

The Power Platform Team does not provide individual access to Environments. PPT will use Microsoft Entra Security Groups to apply a role-based method for applying access to Power Platform Environments. This provides the user base with self-governance of access, while also providing Microsoft best-practice security for environments.

## Security Group Allocation

How to Create Security Groups for Power Platform

There should be a minimum of 3 groups created for a Sandbox or Development environment (this may vary based on needs and requests over time, especially when using Dataverse):

* Maker Group
  + Owners: Supplied via request (csv file) by the environment requestors.
  + Members: Supplied via request (csv file) by the environment requestors.
* Admin Group
  + Owners: PPT Team and Environment owning (IS THIS CORRECT – DO WE GIVE SYS ADMIN TO CLIENT?)
  + Members: None
* User Group
  + Owners: Supplied via request (csv file) by the environment requestors.
  + Members: Supplied via request (csv file) by the environment requestors.

## Step 2: Create Environment

1. Login into Power Platform Admin Center: <https://gcc.admin.powerplatform.microsoft.us/?l=en-US>
2. In the Power Platform admin center, click Environments on the left nav/tool bar

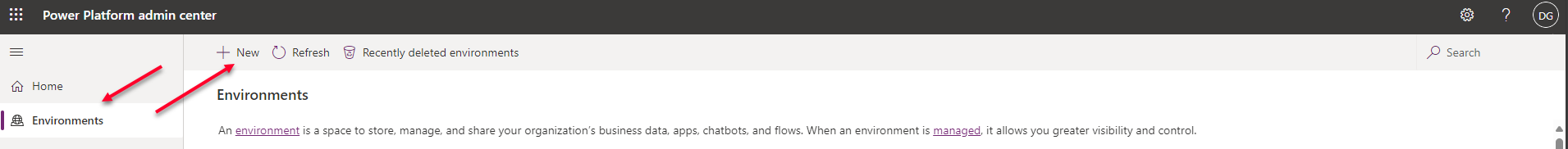


Figure 18

1. Click *New* to create a new environment (a New environment form comes up on the right side of the page)

Figure 19

1. Fields are filled out as follows:
   * New environment form:
     + **Name**: *[BU]-[APP]-Prod or [BU]-[APP]-Test*
       - Example: IT-EOPS-SPO-Prod / IT-EOPS-SPO-Test
     + **Region**: *GCC Default*
     + **Type**: *Production*
     + **Purpose**:
     + **Add a Dataverse data store?**: *Yes*
     + Click the *Next* button (which will bring up the Add Dataverse form)
   * Add Dataverse form:
     + **Language**: *English (United States)*
     + **Currency**: *USD ($)*
     + **Security group** (click + Select): *None*
     + **URL** (click here): *[bu]-[app]-prod (or [bu]-[app]-test) \*All lower case*
       - Example: it-eops-spo-prod or it-eops-spo-test
     + **Enable Dynamics 365 apps?**: *No*
     + **Deploy sample apps and data?**: *No*

|  |  |
| --- | --- |
| Figure 20 | Figure 21 |

## Step 3: Settings

Once you have created the environment, open the environment

1. If you are not already in, login into Power Platform Admin Center: <https://gcc.admin.powerplatform.microsoft.us/?l=en-US>
2. In the Power Platform admin center use the *Search* or browse to find the Power Platform environment you just created in Step 2.

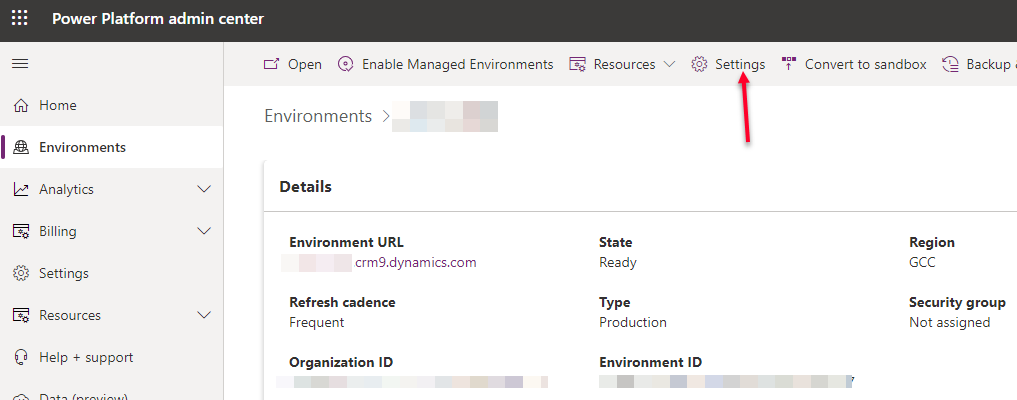


Figure 22

1. In the Details screen, in the upper tool bar, click on *Settings* to open up the Settings panel.

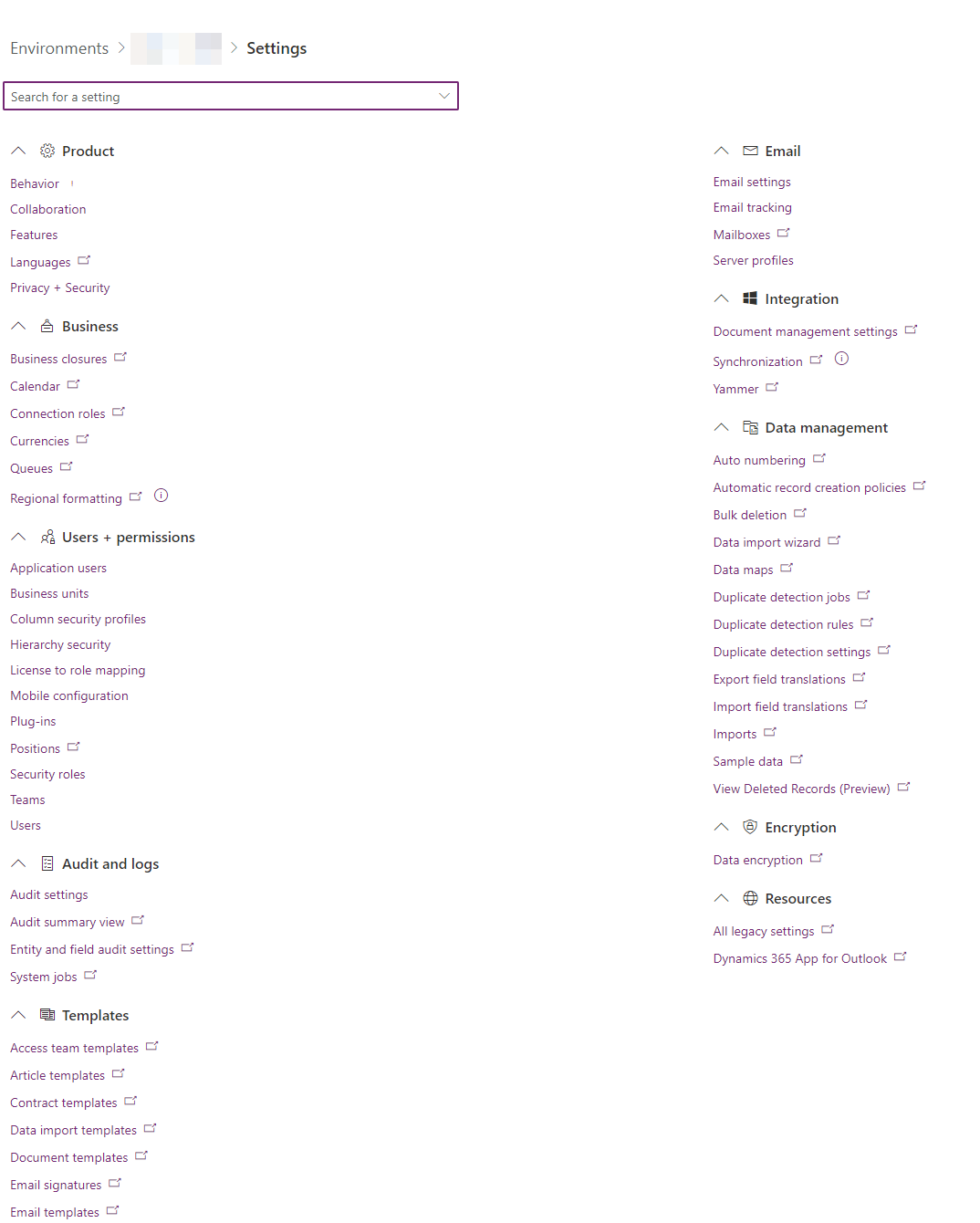


Figure 23

* 1. Under *Product* >
     1. *Behavior*
        1. Make no changes – accept all default settings.
     2. *Collaboration*
        1. Make no changes – accept all default settings.
     3. *Features*
        1. Make all changes as found in Figure #. Of note:
           1. **Allow canvas editors to insert the Copilot answer component, which allows users to receive an AI-powered answer to a predefined data query:** *Turn Off (see figure #: A)*
           2. AI Builder:

**Enable the usage of AI Builder model types that are in preview***: Turn Off* *(see figure #: A)*

* + - * 1. AI Prompts:

**Enable the AI prompts feature in Power Platform and Copilot Studio:** *Turn Off (see figure #: A)*

* + - * 1. Natural language grid and view search

**Find your data in model-driven app views with the help of Copilot.**

*No one*

* + - * 1. AI insight cards:

**Record summaries and other Copilot insights will appear on main forms**

*Turn Off*

* + - * 1. Power Automate Process Mining:

**Enable production ready preview features for Power Automate Process Mining.**

*Turn Off*

* + - * 1. Embedded Content:

**Power BI**: *Turn on* *(see figure #: B)*

* + - * 1. Hosted RPA:

**Enable hosted machine groups**: *Turn Off* *(see figure #: C)*

**Enable work or school accounts for hosted machine groups**: *Turn Off* *(see figure #: C)*

* + - * 1. Search

**Dataverse search**: *Turn On* *(see figure #: D)*

**Single Table Search Option**: *Turn On* *(see figure #: D)*

* + - * 1. Delete disabled users

**Enable delete disabled users**: *Turn On* *(see figure #: E)*

* + 1. *Privacy + Security*
       1. Privacy Preference
          1. **Show privacy statement link for this organization**: *Turn On* *(see figure #: A)*
          2. **Privacy statement URL**:[*https://www.irs.gov/privacy-disclosure/irs-privacy-policy*](https://www.irs.gov/privacy-disclosure/irs-privacy-policy) *(see figure #: B)*
          3. **Default action to take when an error occurs**:

Choose > *Never send an error report to Microsoft* *(see figure #: C)*

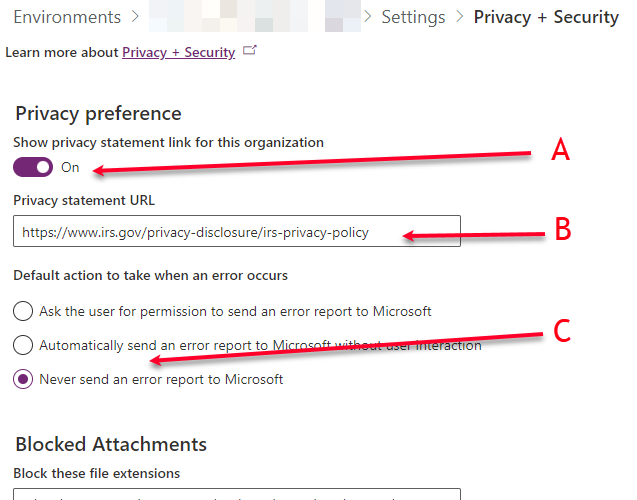


Figure 24

* 1. Under *Audit and Logs* >
     1. *Auditing*
        1. **Start Auditing**: *check on* *(see figure #: A)*
        2. **Log Access**: *check on* *(see figure #: A)*
        3. **Read Logs**: *check on* *(see figure #: A)*

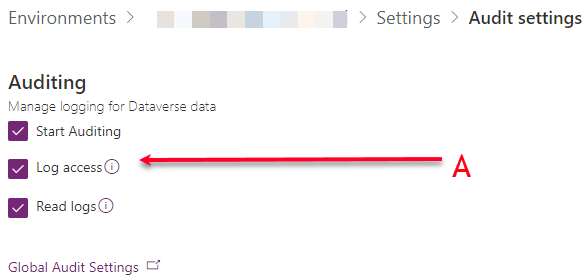


Figure 25

* + - 1. **Retain these logs for:** 5 Years = 1825 Days
         1. \*\* NOTE \*\* You will need to wait up to 24 hours after creating the Environment for this Field to become available, so you will need to ensure you go back in the next day to set this field!
         2. Once you have waited long enough, go back into this section and you will now see this field (Figure 24).

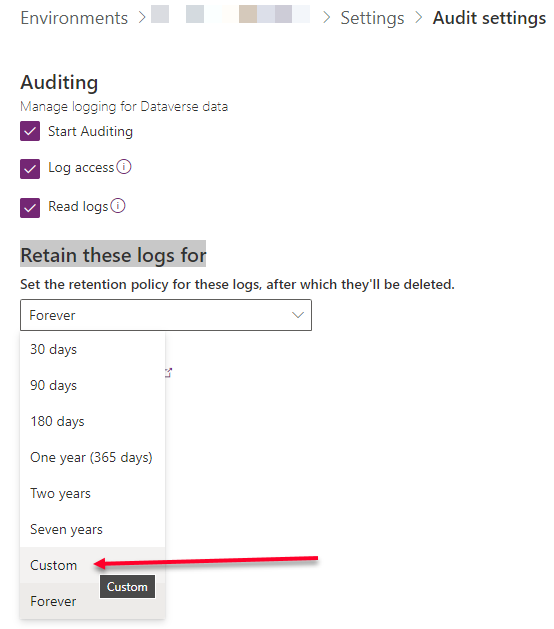


Figure 26

* + - * 1. From the drop-down, select Custom, and enter 1825 (days)

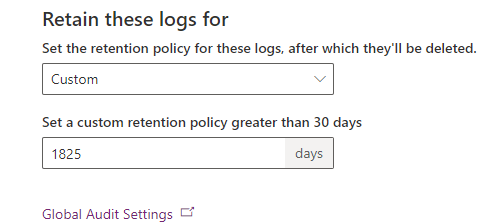


Figure 27

* 1. Under *Users + Permissions* >
     1. Teams
        1. Create team  
           This first team is the Power Platform Team Admins.
           1. **Team Name:** PP Tenant Admins
           2. **Description:** Power Platform role group covering tenant wide Power Platform admins (used to assign admin rights over all environments for IT support)
           3. **Business unit:** <bu name>-<app>-prod (all lowercase)

Example: sbse-transmittal-sandbox

* + - * 1. **Administrator:** <yourself as PP Admin> (currently your boad account)
        2. **Team type:** Microsoft Entra ID Security Group
        3. **Group name:** CLOUD USER M365 MPP IT EOPS PP ADMINS
        4. **Membership type:** Owners
        5. **Role:** System Administrator
      1. Create team
         1. **Team Name:** CLOUD M365 MPP <BU> PROD <APP NAME> USER  
            Should be the same name as defined in *Step 1: Create User Security Group*

Example: CLOUD M365 MPP DEV [BU] [SOL] USER

* + - * 1. **Description:** Users in the <BU> <APP> Sandbox environment
        2. **Business unit:** <bu name>-<app>-prod (all lowercase)  
           Should be the same as the URL entered in the Dataverse Form when creating the Environment.

Example: [bu]-[app]-sandbox

* + - * 1. **Administrator:** <yourself as PP Admin> (currently your boad account)
        2. **Team type:** Microsoft Entra ID Security Group
        3. **Group name:** CLOUD M365 MPP DEV [BU] [SOL] USER  
           Should be the same name as defined in *Step 1: Create User Security Group*
        4. **Membership type:** Members
        5. **Role:** Basic user

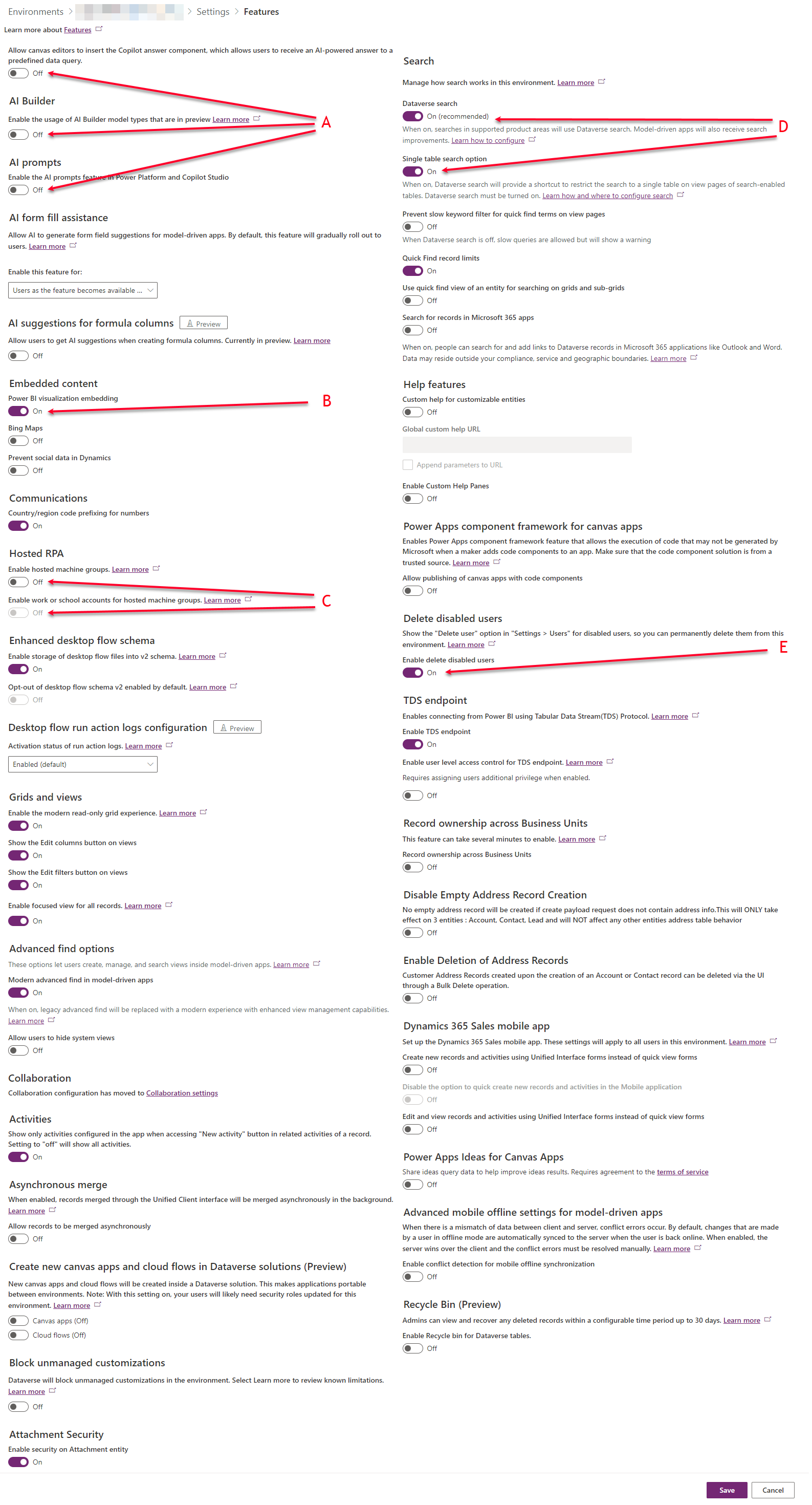
## Step 4: Add to Proper Policy

1. Open Power Platform Admin Center
   * Policies > Data Policies
   * Add non-Dataverse environments to: Baseline
   * Add Dataverse environments to: Default Plus Dataverse
   * Add SQL approved environments to: SQL plus Dataverse
   * Add Oracle plus Dataverse to: Oracle plus Dataverse

## Step 5: Create Approval Tables

This is only necessary for those environments using Approval Microsoft built-in Approvals

1. SAM CAN ENTER THE STEPS Import and run flow to create Approvals Tables



# How to Find and Replace the Owner of a Power App

This may be done using the COE (Center Of Excellence) for Power Platform.

1. Open the Maker portal for IRS tenant: <https://make.gov.powerapps.us/>
2. Navigate to the ***IT-EOPS-COE-Prod*** environment (A)
3. Open the ***Apps*** (B) section and select ***All*** (C)

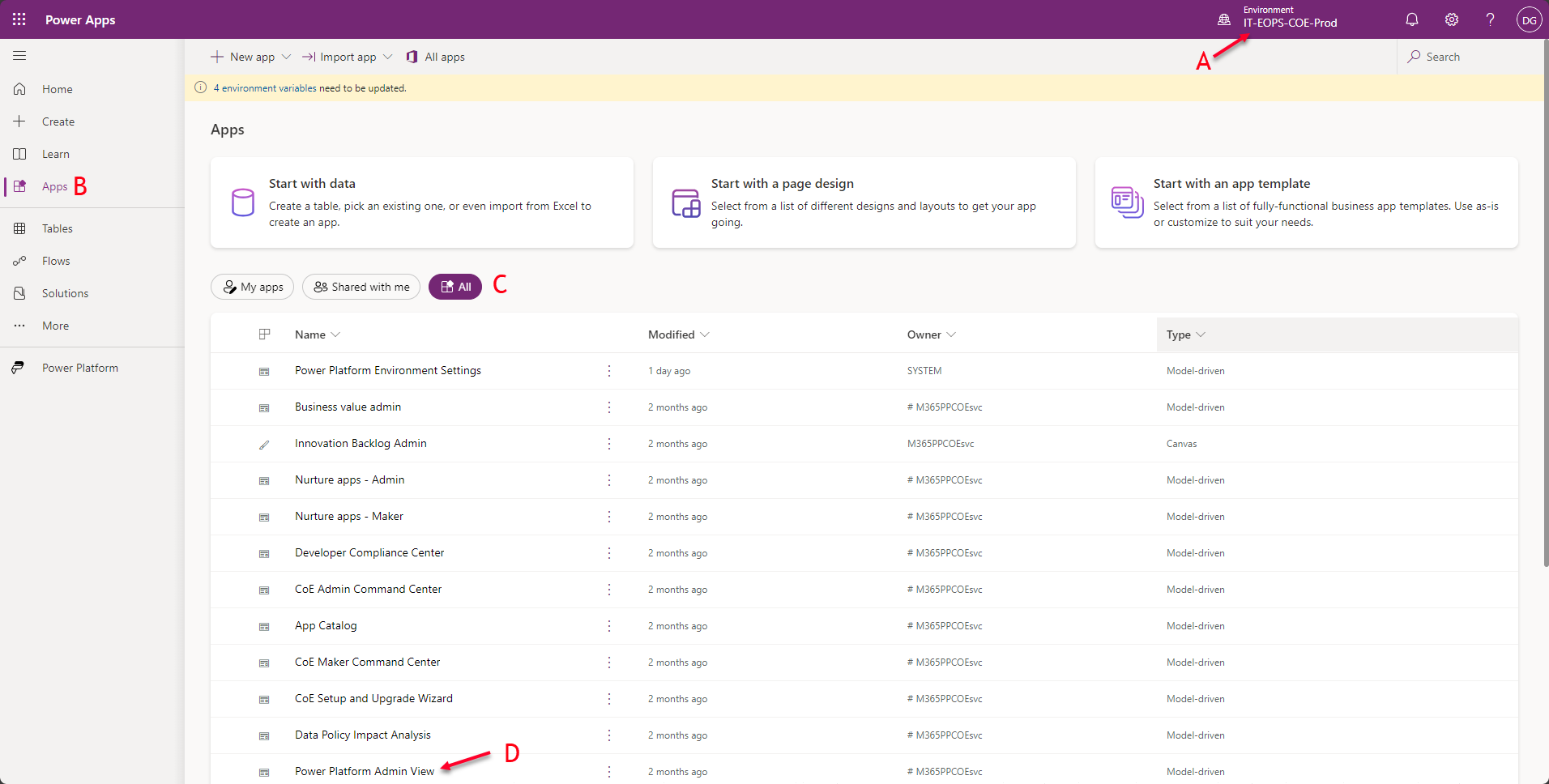


Figure 28

1. Open the ***Power Platform Admin View*** (D).

## Find the Power App ID

There are two primary ways to find the ID of an application.

1. The
2. F
3. F
4. F
5. F
6. f

# Power Platform Pipelines

## Summary of Steps:

* Create a new Environment for the Host
* Create a specific Pipeline User Group for the pipeline
* Add Environments to the Pipeline
* Add Pipelines that include the environments

## How to Create a Pipeline Host

Create a new Environment using How to Add a Production And Test Environment instructions.

### Summary of Steps

* Must be a Production Environment.
* Must be Dataverse enabled.
* Must be Dynamics 365 App enabled.
* Must be placed into the Default Plus Dataverse Data Policy.

1. Created Sandbox (should be done prior to this)
   1. Ensure Maker Group is there
2. Created Test (should be done prior to this)
   1. Ensure same Maker Group from Sandbox is here with same Maker rights
3. Created the Host
   1. Added Dynamics 365 Power Pipelines to the Host environment
   2. Did the settings
4. Inside the Host – Pipelines
   1. Add Environment: Sandbox
   2. Add Environment: Test
   3. Create new Pipeline
      1. Associate with Sandbox
      2. Add new Deployment Stage
         1. Deploy to test
         2. Share with NEW Team à add the Maker Group from Sandbox environment
   4. Go back into the HOST environment, and see that the Maker Group from the step above has been added – give them the “deployment pipeline user” security role ONLY.
   5. Navigate back into the “Create new Pipeline” section to find out pipeline and “Share” with the group we just created and gave the “deployment pipeline user”.

### Step 1: Ensure the Pipeline objects are Set

* Every pipeline should consist of a Sandbox (Dev), Test, and Production environment.

### Step 2: Create the Host Environment

With the ***following exceptions***, perform the Environment creation process laid out in section: ***How to Add a Production And Test Environment***

* Step 2: Create Environment
  + New environment form:
    - **Name**: *HOST-[BU]-PIPELINE*
      * Example: HOST-IT-PIPELINE
    - **Region**: *GCC Default*
    - **Type**: *Production*
    - **Purpose**: *Pipeline host for HOST-[BU]-PIPELINE in support of all pipelines for that BU.*
    - **Add a Dataverse data store?**: *Yes*
    - Click the *Next* button (which will bring up the Add Dataverse form)
  + Add Dataverse form:
    - **Language**: *English (United States)*
    - **Currency**: *USD ($)*
    - **Security group** (click + Select): *None*
    - **URL** (click here): *host-[bu]-pipeline \*All lower case*
      * Example: host-it-pipeline
    - **Enable Dynamics 365 apps?**: *Yes*
    - **Deploy sample apps and data?**: *No*
* Step 3: Settings
  + Under Users + Permissions >
    - Teams
      * Create team  
        This first team is the Power Platform Team Admins.
        + **Team Name:** *PP Tenant Admins*
        + **Description:** *Power Platform role group covering tenant wide Power Platform admins (used to assign admin rights over all environments for IT support)*
        + **Business unit:** *host-[bu]-pipeline*
        + **Administrator:** *<yourself as PP Admin> (currently your boad account)*
        + **Team type:** *Microsoft Entra ID Security Group*
        + **Group name:** *CLOUD USER M365 MPP IT EOPS PP ADMINS*
        + **Membership type:** *Owners*
        + **Role:** *System Administrator*

### Step 3: Add Dynamics 365 apps to the Host environment.

1. Login into Power Platform Admin Center: <https://gcc.admin.powerplatform.microsoft.us/?l=en-US>
2. Open the Host environment you just created.
3. In the left side Power Platform navigation area, expand the ***Resources*** section and click on the ***Dynamics 365 apps*** (see figure XXX).

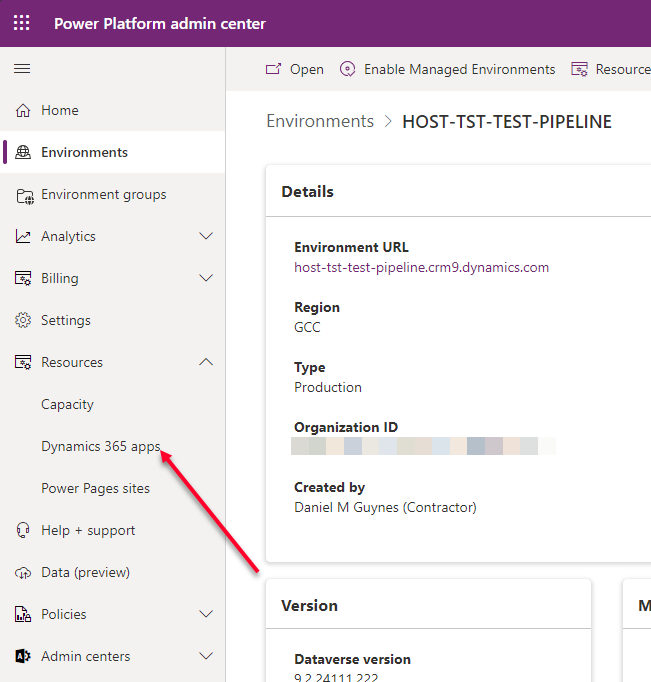


Figure 29

1. When the Dynamics 365 app page opens, scroll down to find Power Platform Pipelines, click on the … and select to Install (see Figure XXX).



Figure 30

1. Under the ***Select and environment \****, click the drop down and scroll down to select the Host environment that you created (see Figure XXX)
2. Check the ***I agree to the terms of service*** check box and click on the Install button (see Figure XXX).

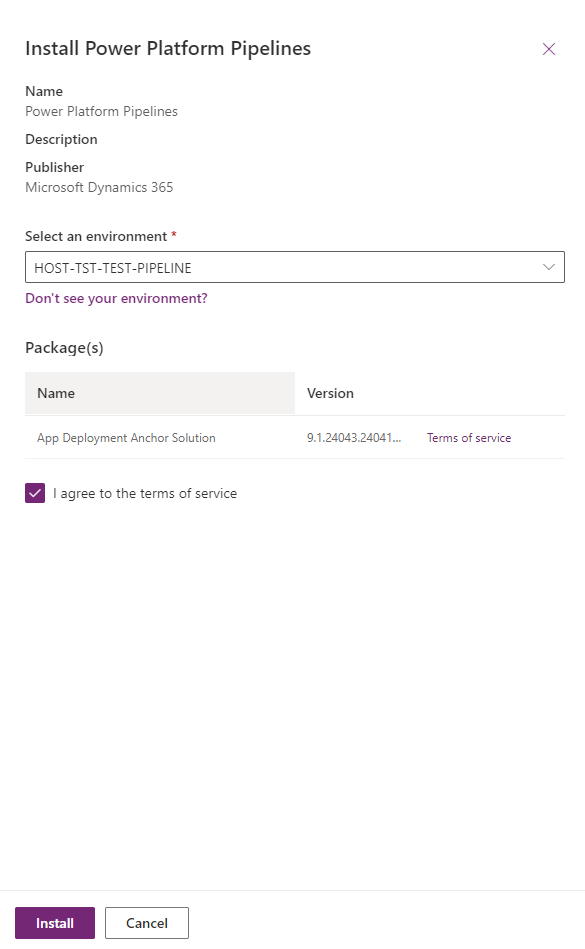


Figure 31

1. This will take time. Once installed proceed to the next step.

## How to Create a Pipeline

### Summary of Steps

* Add Environments to the Host
* Create a Pipeline to attach the Environments to a specific Pipeline
* Create the Deployment Stages
* Finalize Security for the Pipeline

### Step 1: Open the Host Power Platform

1. Navigate to you’re the Power Platform Admin center: [Environments | Power Platform admin center](https://gcc.admin.powerplatform.microsoft.us/environments).
2. Search and pull up the Host environment.
3. Click on the ***Environment URL***, or navigate directly to the environment URL: *host-<bu>-pipeline.crm9.dynamics.com*.
   1. \*\* NOTE \*\* If you are presented with a list of Dynamics 365 apps, select the Power Platform Pipelines.

### Step 2: Add Environments

You need to add each Environment of the Pipeline before creating the Pipeline.

1. On the left side navigation pane, select ***Environments*** (see Figure XXX : A).
   1. \*\* NOTE \*\* (see Figure XXX : C) is the list of existing environments.

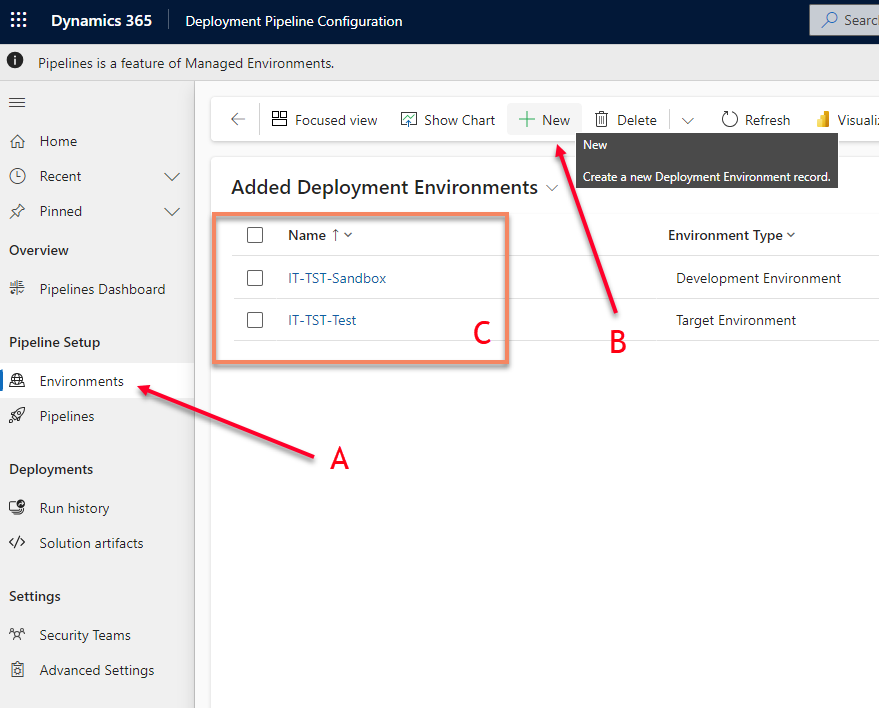


Figure 32

1. Select ***+ New*** to enter a new Environment (see Figure XXX : B).
2. In the New Deployment Environment pane (see Figure XXX) enter the data for each of the 3 environments (Sandbox, Test, Prod) as follows:
   1. Name: This should be the same name as the Environment
   2. Owner: will default to the person entering the information.
   3. Environment Type: for each environment it should be as follows (see arrow in Figure XXX):
      1. Sandbox: Development Environment
      2. Test: Target Environment
      3. Prod: Target Environment
   4. Environment ID: The ID of the environment
   5. Error Message: <leave blank<
   6. Description: enter a basic description

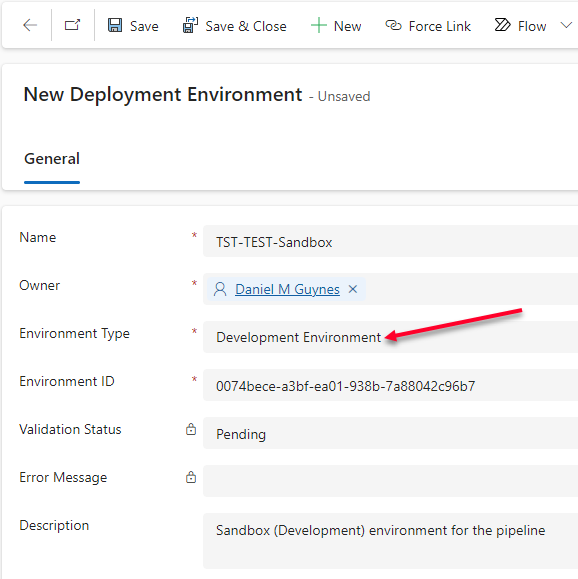


Figure 33

### Step 3: Create New Pipeline

This step can only be performed once the Environments are added from Step 2. The first step is creating the pipeline definition, and the next step (Step 4) defines the pipeline

1. On the left side navigation pane, select ***Pipelines*** (see Figure XXX : A).
   1. \*\* NOTE \*\* (see Figure XXX : C) is the list of existing pipelines.

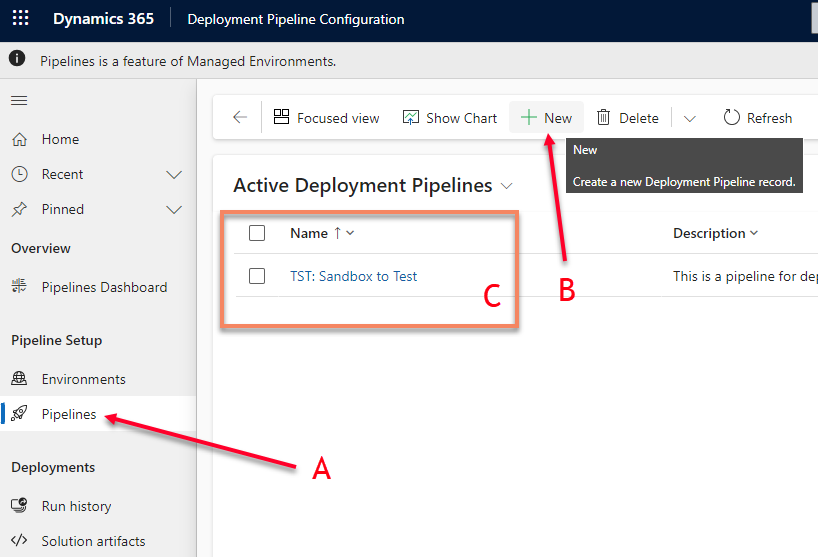


Figure 34

1. Select ***+ New*** to enter a new Pipeline (see Figure XXX : B).
2. In the New Deployment Environment pane (see Figure XXX) enter the data for each of the 3 environments (Sandbox, Test, Prod) as follows:
   1. Name: It is recommended to name the Pipeline the descriptive name of the pipeline as follows:  
      *<Sandbox Environment Name> à <Test Environment Name> à <Prod Environment Name>*
   2. Description:  
      *This is the deployment pipeline to go from:  
      IT-TST-TEST-Sandbox --> IT-TST-TEST-Test and then from   
      IT-TST-TEST-Test --> IT-TST-TEST-Prod*
   3. Owner: This will default to you.
   4. AI deployment notes (U.S. only): *Enabled*
   5. Allow redeployments of older versions: *Enabled*

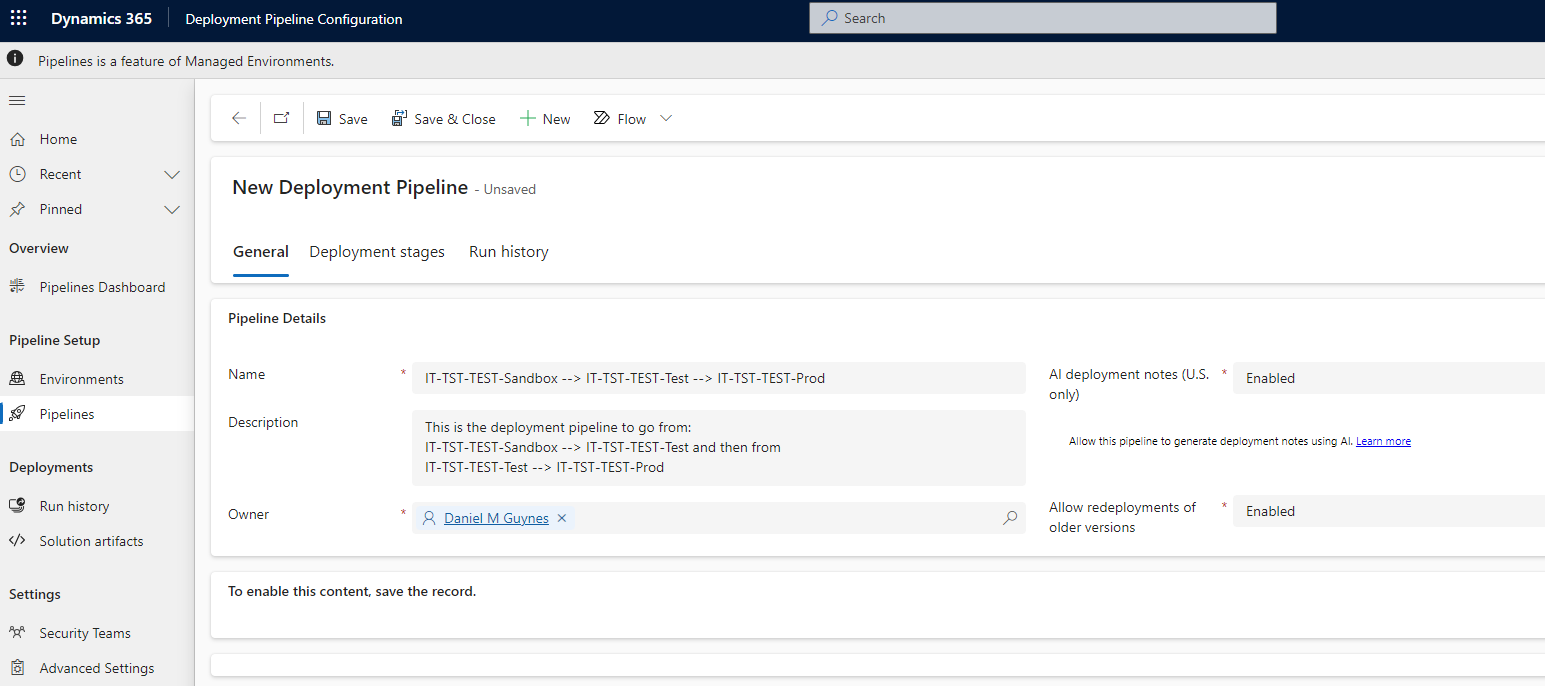


Figure 35

1. Click ***Save*** to save the pipeline definition – you must save it before the next step

### Step 4: Associate the Pipeline with the Sandbox Environment

Once the Pipeline has been defined, you need to attach that pipeline to the Sandbox that the Pipeline will derive from.

1. Once saved, you will see a new section below the Pipeline definition (see Figure XXX). Click the “***Add Existing Deployment Environment***”.

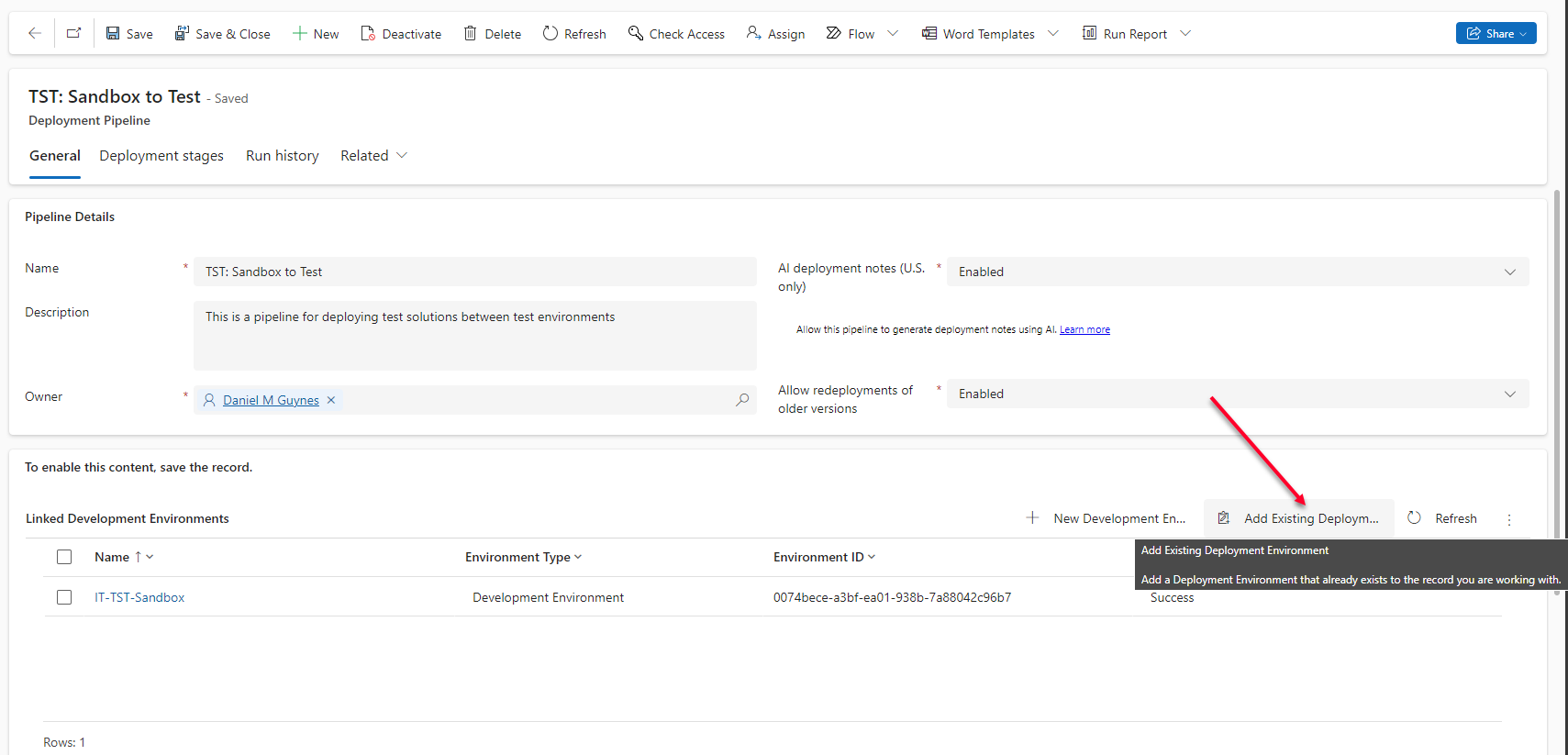


Figure 36

1. In the side data entry panel (**Lookup Records**), select the Sandbox you wish to attach the pipeline to (see Figure XXX). By doing this, this pipeline will be associated only with that sandbox environment.  
   \*\* NOTE \*\* It is possible to have the pipeline attached to multiple Sandbox environments. For instance, if you have multiple solutions from multiple Sandbox environments into a single Test and Prod environment to support a “microservice” style development environment.

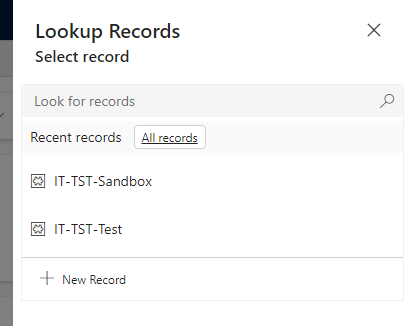


Figure 37

### Step 5: Create the Deployment Stages (Sandbox to Test)

1. Still in the Pipeline, select the ***Deployment stages*** tab (see Figure XXX A).

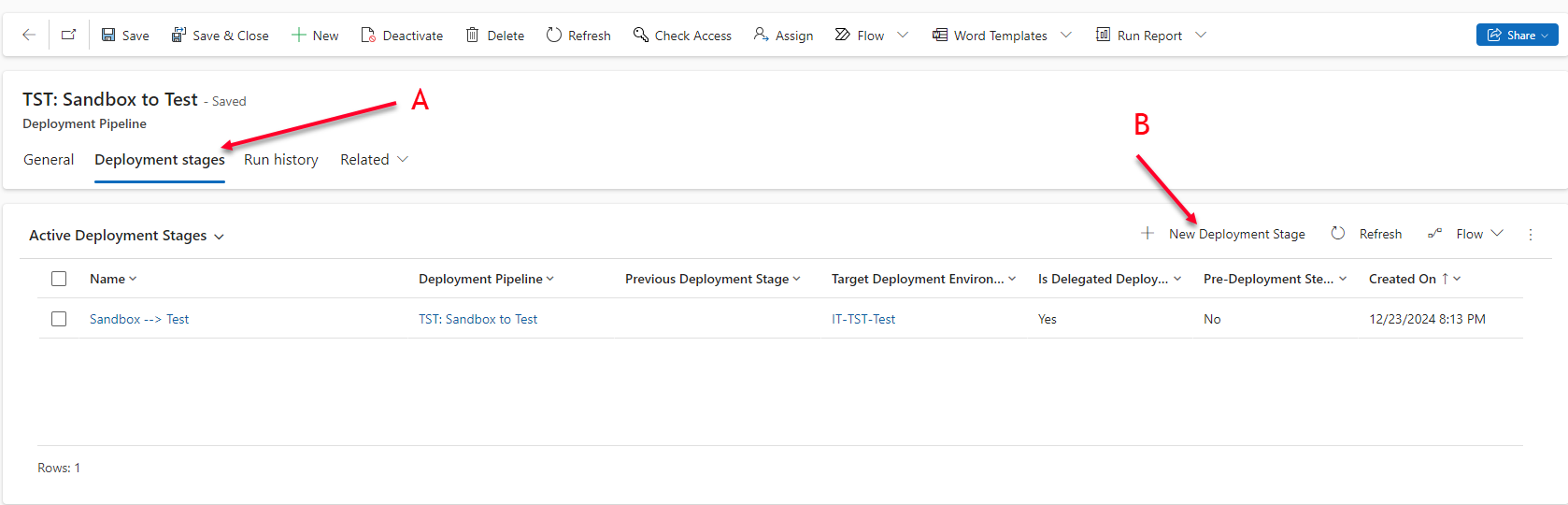


Figure 38

1. In the ***Deployment stages*** pane, select the ***+ New Deployment Stage*** (see Figure XXX B).
2. For the new Deployment stage pane (Figure XXX), enter the information for the deployment as follows:
   1. Name: Sandbox à Test
   2. Owner: Defaults to you
   3. Description: Deployment between Sandbox and Test
   4. Deployment Pipeline: Defaults to the pipeline you are on.
   5. Previous Deployment Stage: leave this blank from Sandbox to Test
   6. Target Deployment Environment ID: Select the Test environment from the selection.
   7. Pre-Export Step Required: Leave blank
   8. Pre-Deployment Step Required: Leave blank
   9. Is Delegated Deployment: Check this box
   10. Delegated Deployment Type: Stage Owner

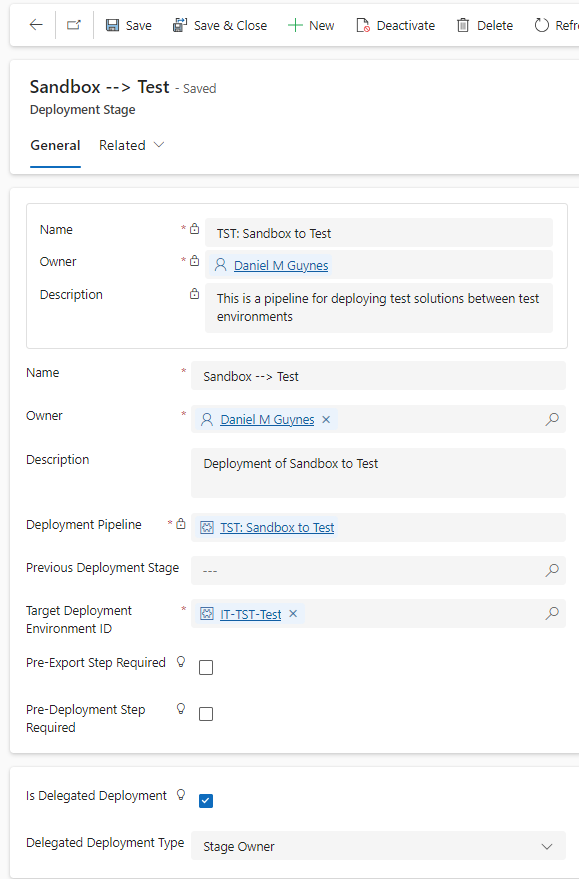


Figure 39

1. Click Save

### Step 6: Create the Deployment Stages (Test to Prod)

1. Follow the same process as Step 5, but when you add a New Deployment Stage, change the field values as follows:
   1. Name: Test à Prod
   2. Previous Deployment Stage: Sandbox à Test (the Stage you created in Step 5)
   3. Target Deployment Environment ID: Select the Prod environment from the selection.
2. Click Save

### Step 7: Setup Security for Pipelines

\*\*NOTE\*\* This section is counter-intuitive to how we set Security up generally for Environments, so pay attention.

1. Create a New Entra Security group (see *Power Platform Basics*
2. *To implement proper Power Platform* application and flow development, the PPT will provide three environments as follows:

* Sandbox (Type: sandbox, unmanaged)
* Test (Type: production, managed)
* Production (Type: production, managed)

# Security for Power Platform Environments

The Power Platform Team does not provide individual access to Environments. PPT will use Microsoft Entra Security Groups to apply a role-based method for applying access to Power Platform Environments. This provides the user base with self-governance of access, while also providing Microsoft best-practice security for environments.

## Security Group Allocation

1. How to Create Security Groups for Power Platform).
   1. This new security group should be titled like the Maker group, but as follows:
      1. CLOUD M365 MPP DEV [BU] [SOL] Pipeline  
         *\*\* NOTE \*\* It was determined that the Pipeline deployers should be separate from the Makers, as you may not wish all your makers to have deployment rights.*
         1. At least two owners should be added to the group, both IRS employees (not contractors).
      2. This Group should be added to the Sandbox, Test, and Prod environments of the pipeline and given the same Security Roles as the Maker group:
         1. Security role(s): Environment Maker, System Customizer

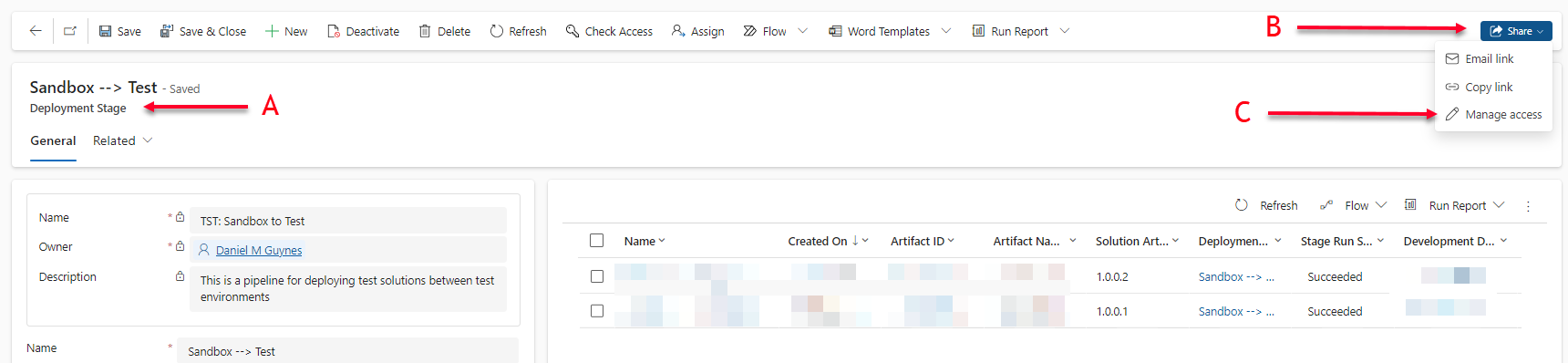


Figure 40

1. Navigate to the ***Deployment Stage*** panel of the pipeline you created (Step 6 above – See Figure XXX: A)
   1. In the upper right, click ***Share*** (See Figure XXX: B)
   2. Under the ***Share*** click ***Manage access*** (See Figure XXX: C).

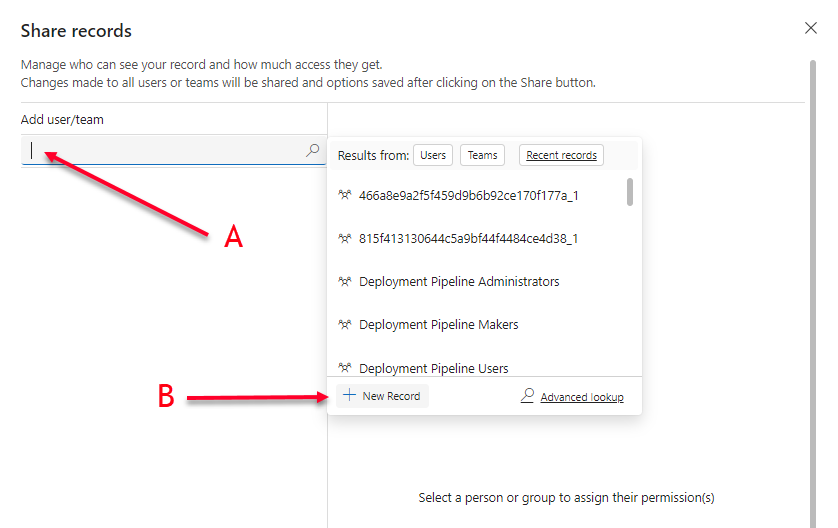


Figure 41

* 1. Click inside of the ***Add user/team*** field and the select ***+ New Record*** from the pop-up (see Figure XXX: A & B). This will replace the pop-up with a new pop-up (see Figure XXX). In the new pop-up click ***Teams***.

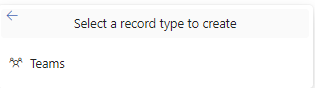


Figure 42

* 1. This will prompt you to leave the page (see Figure XXX), and you will select OK.

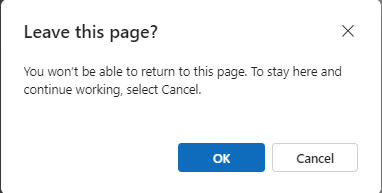


Figure 43

* 1. This will take you to a new screen where you will essentially be adding a new Team to the Host environment like you would normally when creating an environment (see ***Power Platform Basics***
  2. ***To implement proper Power Platform*** application and flow development, the PPT will provide three environments as follows:
* Sandbox (Type: sandbox, unmanaged)
* Test (Type: production, managed)
* Production (Type: production, managed)

# Security for Power Platform Environments

The Power Platform Team does not provide individual access to Environments. PPT will use Microsoft Entra Security Groups to apply a role-based method for applying access to Power Platform Environments. This provides the user base with self-governance of access, while also providing Microsoft best-practice security for environments.

## Security Group Allocation

* 1. How to Create Security Groups for Power Platform and Figure XXX)

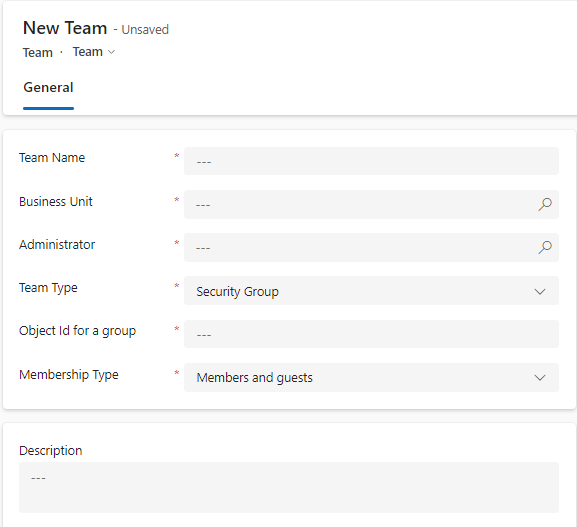


Figure 44

* + 1. **Team name:** Should be the same Entra Group name of the *Pipeline* group for the Sandbox environment that is the basis of this pipeline.
    2. **Description:** Should be a descriptive text about the function of the group.
    3. **Business unit:** should be the default business unit of the host environment that the pipeline belongs.
    4. **Administrator:** Add your OAD account (this may change later to be by a Group)
    5. **Team type:** Microsoft Entra ID Security Group
    6. **Object Id for a group:** Should be the unique GUID of the Entra Group representing the Pipeline group of the Sandbox environment that is the basis of this pipeline.
    7. **Membership type:** Members
    8. Save the record, by clicking by clicking on the save icon on the form.

1. Next Login into Power Platform Admin Center: <https://gcc.admin.powerplatform.microsoft.us/?l=en-US>.
   1. Open the Host environment that you are working with for this pipeline.
   2. Under *Settings à Users + Permissions* > (or you may click on ***See all*** under ***Teams***, within the ***Access*** panel of the Environment home screen), select Teams.
      1. You should see within the list of teams, the *Pipeline* group you “shared” the pipeline with from the above step.
      2. Click on the three dots associated with the *Pipeline* group you just added and click on ***Manage security roles***.
      3. Add **ONLY** the ***deployment pipeline user*** role – and no other role.
2. Now you will need to navigate to the ***Deployment Stage*** panel of the pipeline you created (Step 6 above – See Figure XXX: A) and re-share with the *Pipeline* group and provide ***Read*** permissions only.  
   \*\*NOTE\*\* In the previous step we added a new Team to share with, but did not actually share with the team, just added it … and now we are physically sharing with that team.

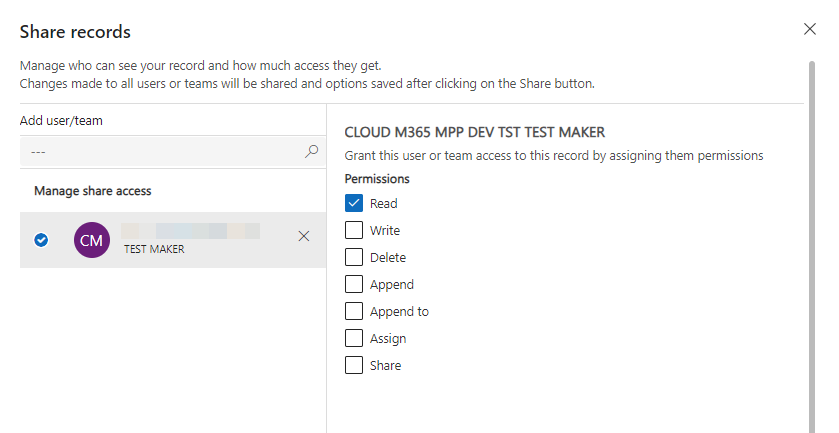


Figure 45

1. Finally, you will need to add the Maker group from the Sandbox to all target environments within the Pipeline (i.e. the Test and Prod environments where the pipeline will deploy the solution.) and provide them with the same security roles: ***Environment Maker***, ***System Customizer*** if you have not already done so.

# How to Change the Owner of a Power App or Power Automate Flow

Note that the process is the same for the App as with the Flow, with the difference being only that instead of selecting ***Apps*** (first bullet of Step 2) you select ***Flows***.

## Summary of Steps

* Navigate to the COE
* Select App
* Add User as Owner (which replaces the existing one)

## Step 1: Navigate to COE

* Navigate to: [it-eops-coe-prod.crm9.dynamics.com](https://it-eops-coe-prod.crm9.dynamics.com/)

## Step 2: Locate the Environment

* Click Apps (Figure XXX: A) in the left navigation area.
* Locate the Environment and select it (Figure XXX: B) by clicking on the icon next to it.  
  \*\* NOTE\*\* It may take some time for all of the apps in the environment to load, so you may need to wait before proceeding to the next bullet in this step.
* From the list of Apps, locate the App within the Environment and click on the name of the App (Figure XXX: C).

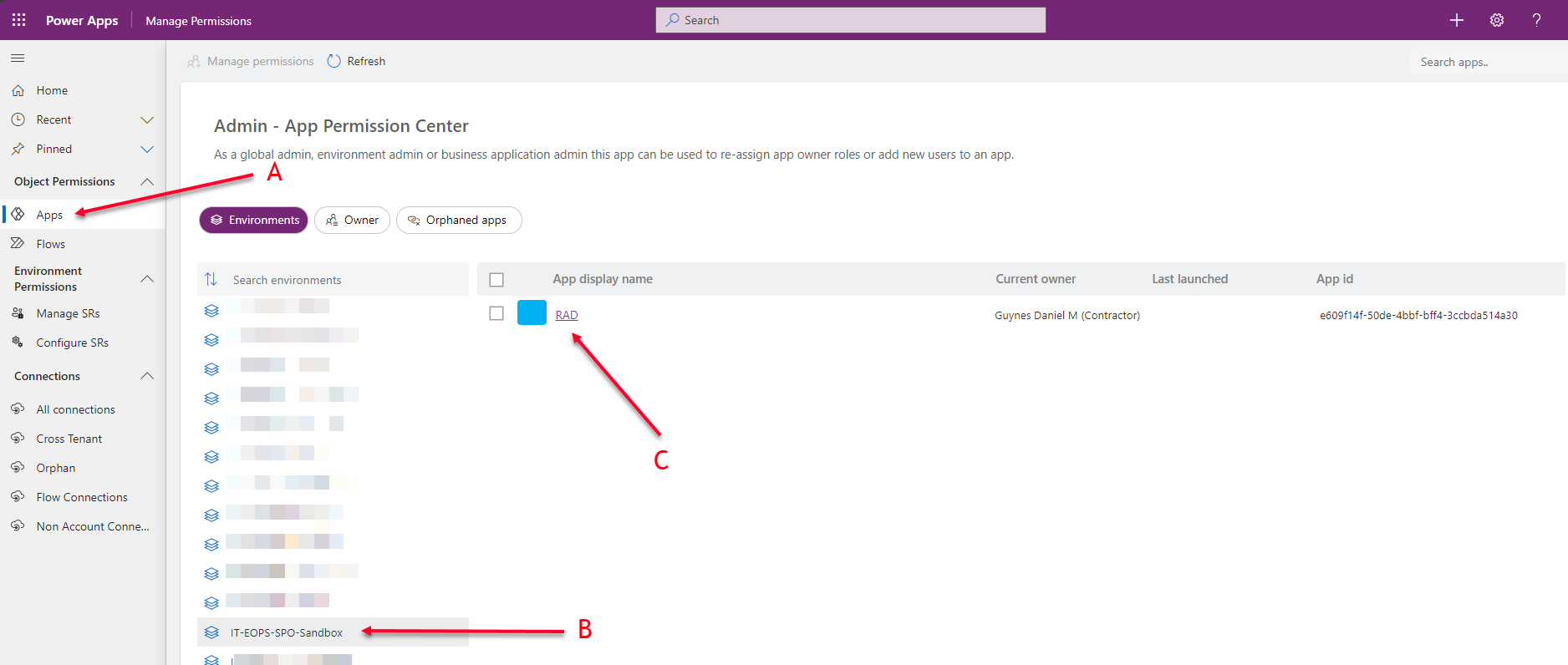


Figure 46

## Step 3: Add the new Owner

* Figure XXX E shows the current Owner of the App, and after you have completed this, will show the new owner.
* Click on ***Add new users*** (Figure XXX: A) which will open a side pane to the right to add your users.
* Start entering the name of the user you wish to add into the people picker ***Select user*** field (see Figure XXX: B) until you are presented with a drop down with the user you wish to add, and select them from the drop down.
* From the ***Select user role*** drop down field, select Owner (Figure XXX: C).
* Finally, click the ***Add user*** button at the bottom of the pane (Figure XXX: D) to replace the current owner with your new owner.

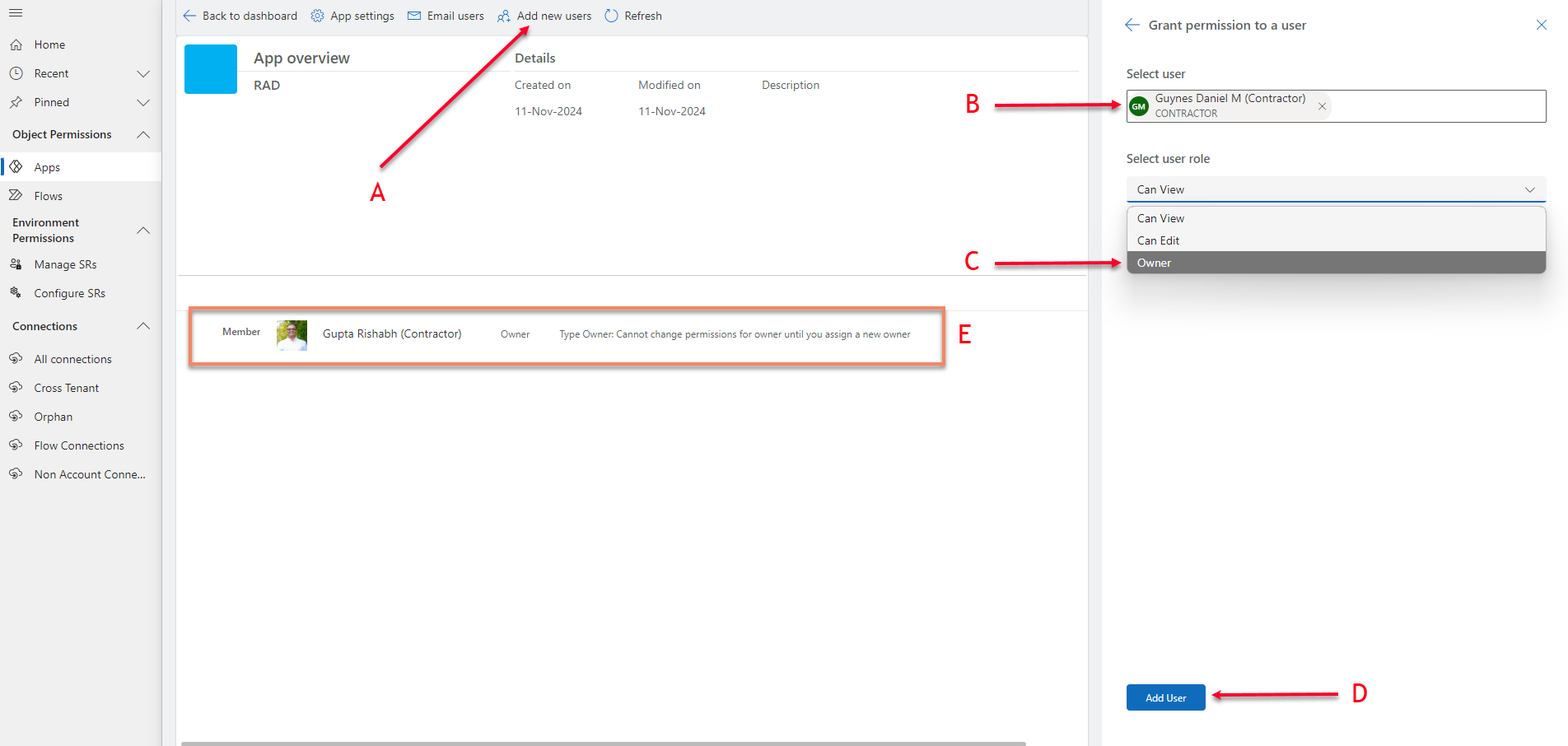


Figure 47

# How to Find an Entra Group Attached to an Environment

## Summary of Steps

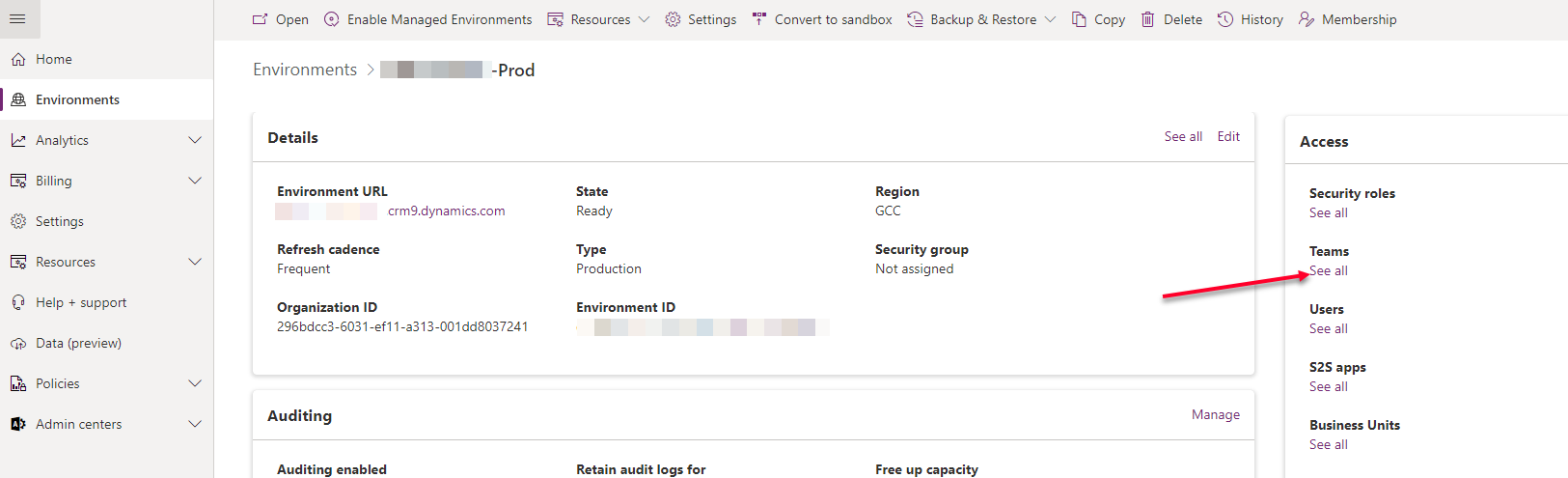
* Navigate to the Environment
* Find the Team that the Entra Group is attached to, and identify the Entra Group ID

## Step 1: Navigate to Environment

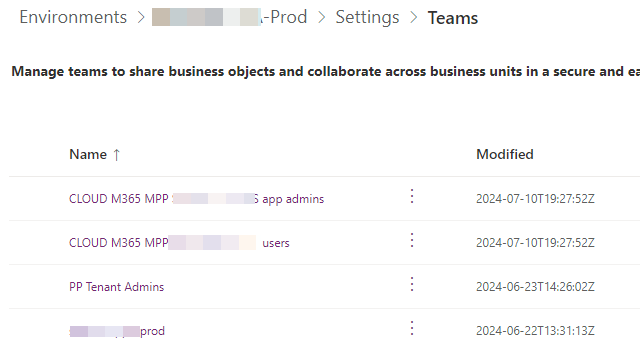
* Login into Power Platform Admin Center: <https://gcc.admin.powerplatform.microsoft.us/?l=en-US>
* In the Power Platform admin center, click Environments on the left nav/tool bar
* Using the Search in the upper right of the page, search for the environment you are looking for.
* Click on the Environment to open up the environment details.

## Step 2: Identify Entra Group ID

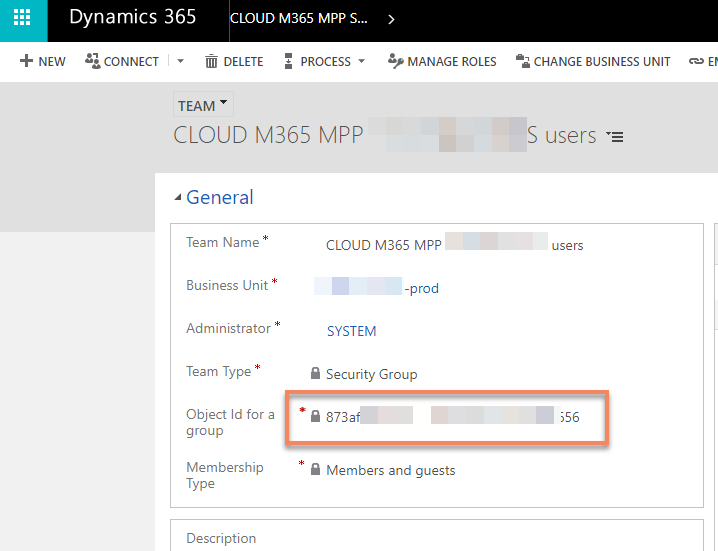
* Under the Settings, beneath Teams click on See all.



* To find the unique identity to the Entra group, click the Team name to open the Dynamics 365 profile

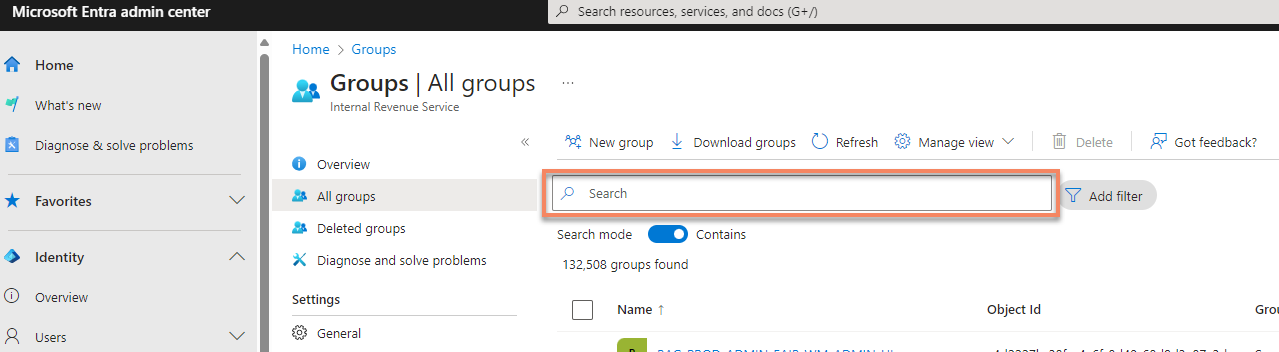


* In the Dynamics 365, under the General section, copy and save the “Object Id for a group” (Group GUID) value.



## Step 3: Find Group in Microsoft Entra

* With the Group GUID, login into Microsoft Entra: <https://entra.microsoft.com/>.
* On the left Tool bar select Identity à Groups à All groups (Figure 3).
* In the Groups | All groups panel, along the top of the pane, enter the Group GUID into the search box.



* This should bring up the unique Entra Security group associated with an Environment Team.
  + Make any changes with the Group as needed.

# Standard Processes

SOPs we need to create:

* Implementation of a Sandbox environment
* Implementation of a Test and Prod Environments
* Creation and Editing of a DataGateway
* Implementation of a Connection using a datagateway
  + SQL
  + Oracle
  + POSTgres
* Creation and implementation of a Custom Connector
* How to Find the owner of an App, a Form, or an Environment
* How to identify an Entra Security Group ID
* How to Create or Edit a Pipeline Host
* How to create or edit a Pipeline
* PPT Spring Scrum cycle definition

## Development Environments

## Sandbox (Group Development) Environments

### Security Groups / Teams

The Sandbox environment should have four core groups added when created:

* PP Tenant Admins
  + This is reserved ONLY for Power Platform Admins (CLOUD USER M365 MPP IT EOPS PP ADMINS) – and should be set to the Owners.
    - Security Roles: System Administrators
* Maker Group
  + The list of Members should be provided by the client.
  + The Owners should be provided by the client and should consist of at least two persons from the client.
    - Security Roles: Environment Maker; System Customizer
* Admin Group
  + The list of Members should be provided by the client.
  + The Owners should be provided by the client and should consist of at least two persons from the client.
    - Security Roles: System Administrators
* User Group
  + The list of Members should be provided by the client.
  + The Owners should be provided by the client and should consist of at least two persons from the client.
    - Security Roles: Basic User

## Test Environments

### Security Groups / Teams

* PP Tenant Admins
  + This is reserved ONLY for Power Platform Admins (CLOUD USER M365 MPP IT EOPS PP ADMINS) – and should be set to the Owners.
    - Security Roles: System Administrators
* Maker Group - NONE
* Admin Group - NONE
* User Group
  + The list of Members should be provided by the client.
  + The Owners should be provided by the client and should consist of at least two persons from the client.
    - Security Roles: Basic User

## Production Environments

### Security Groups / Teams

* PP Tenant Admins
  + This is reserved ONLY for Power Platform Admins (CLOUD USER M365 MPP IT EOPS PP ADMINS) – and should be set to the Owners.
    - Security Roles: System Administrators
* Maker Group - NONE
* Admin Group - NONE
* User Group
  + The list of Members should be provided by the client.
  + The Owners should be provided by the client and should consist of at least two persons from the client.
    - Security Roles: Basic User

# Standard Reports

Licenses

Power Platform Premium Licenses

Environments

Development (Dev)

Development (Sandbox – Managed)

Test/UAT (Sandbox – Managed)

Production (Production – Managed)

Pipelines

# Standard Operating Procedures

# COE Updates

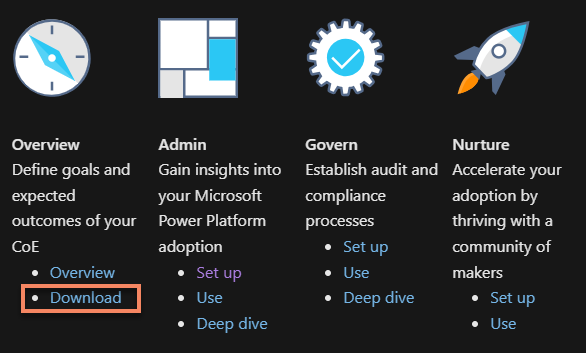
In order to do this we can either COPY the IT-EOPS-COE-Prod, backup the IT-EOPS-COE-Prod into a new environment, or you can do a in-place upgrade.

Whether you copy or back up into a new environment, you will need to create a new environment.

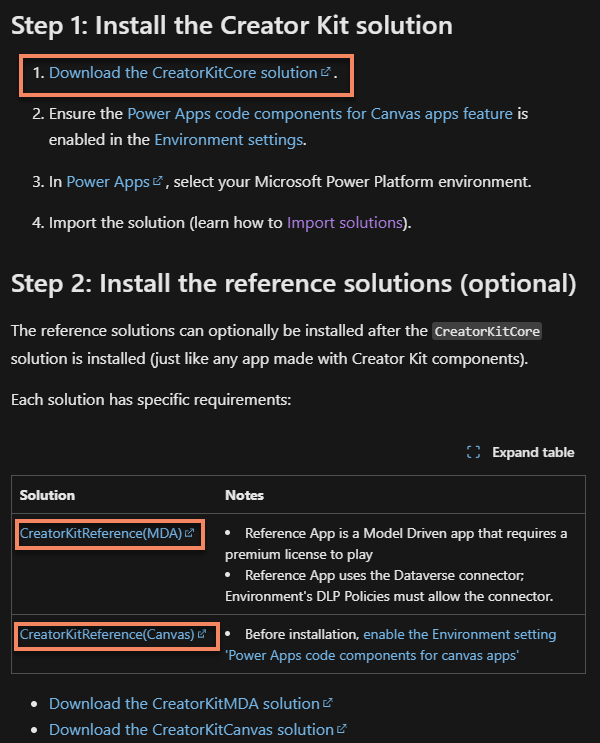
You can then either COPY into the new environment or run a Restore from IT-EOPS-COE-Prod into the new environment.

\*\* NOTE \*\* - You should log in as m365ppcoesvc@irsgov.onmicrosoft.com

1. Go to: [Microsoft Power Platform Center of Excellence Kit - Power Platform | Microsoft Learn](https://learn.microsoft.com/en-us/power-platform/guidance/coe/starter-kit) under Overview click download and download the information (or you can go to: [GitHub - microsoft/coe-starter-kit](https://github.com/microsoft/coe-starter-kit)).



1. Next go to [Set up inventory components - Power Platform | Microsoft Learn](https://learn.microsoft.com/en-us/power-platform/guidance/coe/setup-core-components) to install the creator kit
2. [Set up the Creator Kit - Power Platform | Microsoft Learn](https://learn.microsoft.com/en-us/power-platform/guidance/creator-kit/setup) Download the CreatirKitCore solution
   1. And Import:
      1. CreatorKitReference(MDA) (i.e. CreatorKitReferencesMDA\_1.0.20221205.3\_managed.zip)
      2. CreatorKitReference(Canvas) (i.e. CreatorKitReferencesCanvas\_1.0.20221205.1\_managed.zip)
3. Once those have been done unzip the CoEStarterKit and inside of the CoEStarterKit folder import the CoreComponents solution (i.e. CenterofExcellenceCoreComponents\_4\_43\_managed.zip)



Once you have a backup or copy, you can perform an in-place upgrade.

1. In the main COE import the Creator Kit if it is new
2. Import MDA
3. Import Canvas
4. Unzip the *CoEStarterKit*
   1. Import Core Components (i.e. CenterofExcellenceCoreComponents\_4\_43\_managed.zip)