A picture containing drawing

Description automatically generated

Power Platform Governance Plan Sample



Prepared by: Rishabh Mathur

Date: Wednesday, October 26, 2022

Table of Contents

[1 Welcome 4](#_Toc65527578)

[2 Understanding our tenant 5](#_Toc65527579)

[3 Environments 7](#_Toc65527580)

[3.1 Purpose of Environments 7](#_Toc65527581)

[3.2 Environments in the Contoso tenant 8](#_Toc65527582)

[3.3 Shared Environments 8](#_Toc65527583)

[3.3.1 Contoso Personal Productivity (contosodefault) 8](#_Toc65527584)

[3.3.2 Contoso Power Us​er 9](#_Toc65527585)

[3.3.3 Contoso Pro Dev 12](#_Toc65527586)

[3.4 Trial Environments 13](#_Toc65527587)

[3.5 Custom Environ​ments 14](#_Toc65527588)

[4 Data Loss Prevention (DLP) Policies 18](#_Toc65527589)

[4.1 CONTOSO UltraLo​w (Default Policy) 18](#_Toc65527590)

[4.2 CONTOSO Low (Contoso Power User) 18](#_Toc65527591)

[4.3 CONTOSO Medium (Contoso Pro Dev) 19](#_Toc65527592)

[4.4 CONTOSO Medium​ - Isolated (Custom Environments) 19](#_Toc65527593)

[4.5 Comparing DLP Policies​ 19](#_Toc65527594)

[4.6 Adding New Pre-Built C​onnectors​ 20](#_Toc65527595)

[4.7 Adding Custom Connectors 20](#_Toc65527596)

[4.8 The SAMPLE Connector 21](#_Toc65527597)

[4.9 Custom Policies 21](#_Toc65527598)

[5 ​Environment Roles and Object Sharing 22](#_Toc65527599)

[5.1 Environment Roles 22](#_Toc65527600)

[5.1.1 Environment Maker 22](#_Toc65527601)

[5.1.2 System Administrator 22](#_Toc65527602)

[5.2 Other Environment Roles 23](#_Toc65527603)

[5.3 Service Accounts 23](#_Toc65527604)

[**5.3.1** Getting a Service Account 23](#_Toc65527605)

[**5.3.2** Licensing a Service Account 24](#_Toc65527606)

[**5.3.3** ​​Working as a Service Account 25](#_Toc65527607)

[**5.3.4** Emailing with a service account 25](#_Toc65527608)

[5.4 Object Sharing 26](#_Toc65527609)

[5.4.1 Power App Sharing 27](#_Toc65527610)

[5.4.2 Power Automate Flow Sharing 28](#_Toc65527611)

[5.4.3 Shared Connections 34](#_Toc65527612)

[6 Moving objects between envir​onments 36](#_Toc65527613)

[6.1 Moving a Power Platform solution 36](#_Toc65527614)

[6.2 Moving a Power Apps canvas app 36](#_Toc65527615)

[6.2.1 Saving the file locally 36](#_Toc65527616)

[6.2.2 **​**Using the Export package feature 36](#_Toc65527617)

[6.3 ​Export​ing a Power Automate Flow to another environment 42](#_Toc65527618)

[7 Getting Hel​p 48](#_Toc65527619)

# Welcome

Welcome to the Power Platform Contoso tenant! The Power Platform embodies the Microsoft vision to empower the planet, and our philosophy in CONTOSO is that we want to support citizen and team development within our tenant, meeting that goal while protecting Microsoft assets.

Disclaimer:

Sample document is provided for the purpose of illustration only and is not intended to be used in a production environment. THIS SAMPLE document AND ANY RELATED INFORMATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE. We grant You a nonexclusive, royalty-free right to use and modify the Sample document and to reproduce and distribute the object document form of the Sample document, provided that. You agree: (i) to not use Our name, logo, or trademarks to market Your software product in which the Sample document is embedded; (ii) to include a valid copyright notice on Your software product in which the Sample document is embedded; and (iii) to indemnify, hold harmless, and defend Us and Our suppliers from and against any claims or lawsuits, including attorneys’ fees, that arise or result from the use or distribution of the Sample document.

# Understanding our tenant

The Power Platform Contoso tenant is made up of several environments. Each environment can contain Power Apps, Power Automate Flows, a portal, a Common Data Service (CDS) database and many other types of objects.

A screenshot of a cell phone

Description automatically generated

The Contoso tenant has been configured so you can quickly create powerful productivity solutions and share them with your colleagues.

Your responsibilities in the Contoso tenant:

* **Keep the tenant clean**. Delete your environments, apps, and flows if they are no longer needed.
* **Share wisely**. Watch out for oversharing of your environments, apps, flows, and shared connections​. Read the section on **Object Sharing** to know how to do this right.
* **Protect Contoso data**. Avoid moving data from highly confidential or confidential data sources to non-protected or external storage.
* **Know your data classification**. Use the **Data Classification Wizard** to determine if the data in your solution is Public, General, Confidential or Highly Confidential.
* **You are responsible for sensitive Contoso data**. If your Power Platform objects use Microsoft Confidential or Highly Confidential data, then you are responsible for the handling of that data in accordance with **Contoso Security Policy and Standards**.

# Environments

Environments are containers for objects in the Power Platform. Think of an environment like a Windows folder, used for grouping and securing your objects. When you sign in at powerapps.com or flow.microsoft.com, you’ll see one or more environments in the dropdown list at the upper right. When you select an environment, you’ll be able to see the apps, flows, and other objects that have been shared with you. And, if you are an **Environment Maker​**, you’ll be able to create your own objects.

## Purpose of Environments

Environments are useful for several purposes:

* **Access control** – an administrator of an environment can limit who can create objects like apps or flows in an environment. This is great for teams that want to group their apps in one place. Just be aware that these creators, called makers, can share their objects with people outside the group.
* **Performance** – when an environment is created, it resides in a regional Azure datacenter. Apps, flows, and connections reside here as well. As users run your apps and flows and make data calls through your connections, these interactions are through regional endpoints, which can greatly optimize performance.
* **Application Lifecycle Management (ALM)** – it can be beneficial to have preproduction and production environments. Makers can develop and test in the pre-production environment and export a package, called a Solution, to the production environment.
* **Compliance or tented solutions** – In some cases, you need to isolate a solution so others don’t accidentally gain access to it. Perhaps the data in the application is subject to Sarbanes-Oxley (SOX) provisions or related to a secret project at Microsoft.
* **Connector risk reduction** – The Power Platform uses connectors to access data from services. A tenant administrator can define which connectors are allowed in which environment through Data Loss Prevention (DLP) policies. In this way, access to higher risk connectors can be constrained to approved environments.
* **CDS or Dynamics 365** – an environment can be provisioned with a Common Data Service (CDS) database to easily create database applications. Alternately an environment can be created with a Dynamics 365 org for even more power.
* **Portals** – an environment can have one portal, a powerful way of exposing data and content to internal and external users.

## Environments in the Contoso tenant

At Contoso we have thousands of environments. Some **Shared Environments** have already been provisioned for you by CONTOSO, and are a great place to quickly get your solutions up and running. For test or proof of concept projects that require access to Contoso data, **Trial Environments** can be provisioned within a matter of minutes. For teams that have more specialized requirements, **Custom Environments** can be provisioned with CDS, Dynamics 365, or custom DLP policies.

There are many types and subtypes of environments beyond these logical groupings. To learn more about environments on the Power Platform, visit <https://docs.microsoft.com/en-us/power-platform/admin/environments-overview>.

## Shared Environments

To support integrations, reduce the number of environments needed, and accelerate onboarding, CONTOSO has already created several shared environments that can be used by individuals and teams.

### **Contoso Personal Productivity (contosodefault)**

This is the default environment, formerly known as **Contoso (new default)**. Everyone, including FTEs and contingent staff, has permissions to create apps and flows here. This is also the environment that is used for first party integrations, like creating an app from a SharePoint list.

To reduce risk to Contoso data, we limit the types of connectors you can use in your apps and flows to the **CONTOSO Ultra L​ow Policy**. This policy covers common individual and small team productivity use cases, like working with SharePoint data, sending emails, and having an approval workflow.​

Gaining Access to Contoso Personal Productivity ​​

All Microsoft FTEs, interns, and contingent staff have access to create apps and flows in the Contoso Personal Productivity environment.

To begin, simply go to [www.powerapps.com](http://www.powerapps.com/) and sign in with your MS credentials. On your first visit you’ll automatically be in the Contoso Personal Productivity environment. If you visited another environment during your last session, it will be remembered.

### **Contoso Power Us​er**

While the Contoso Personal Productivity environment covers many use cases, we understand that some power users will have more advanced needs for their apps and flows, like integrating with Microsoft Teams, Azure AD, Azure DevOps, or Power Platform admin functions.

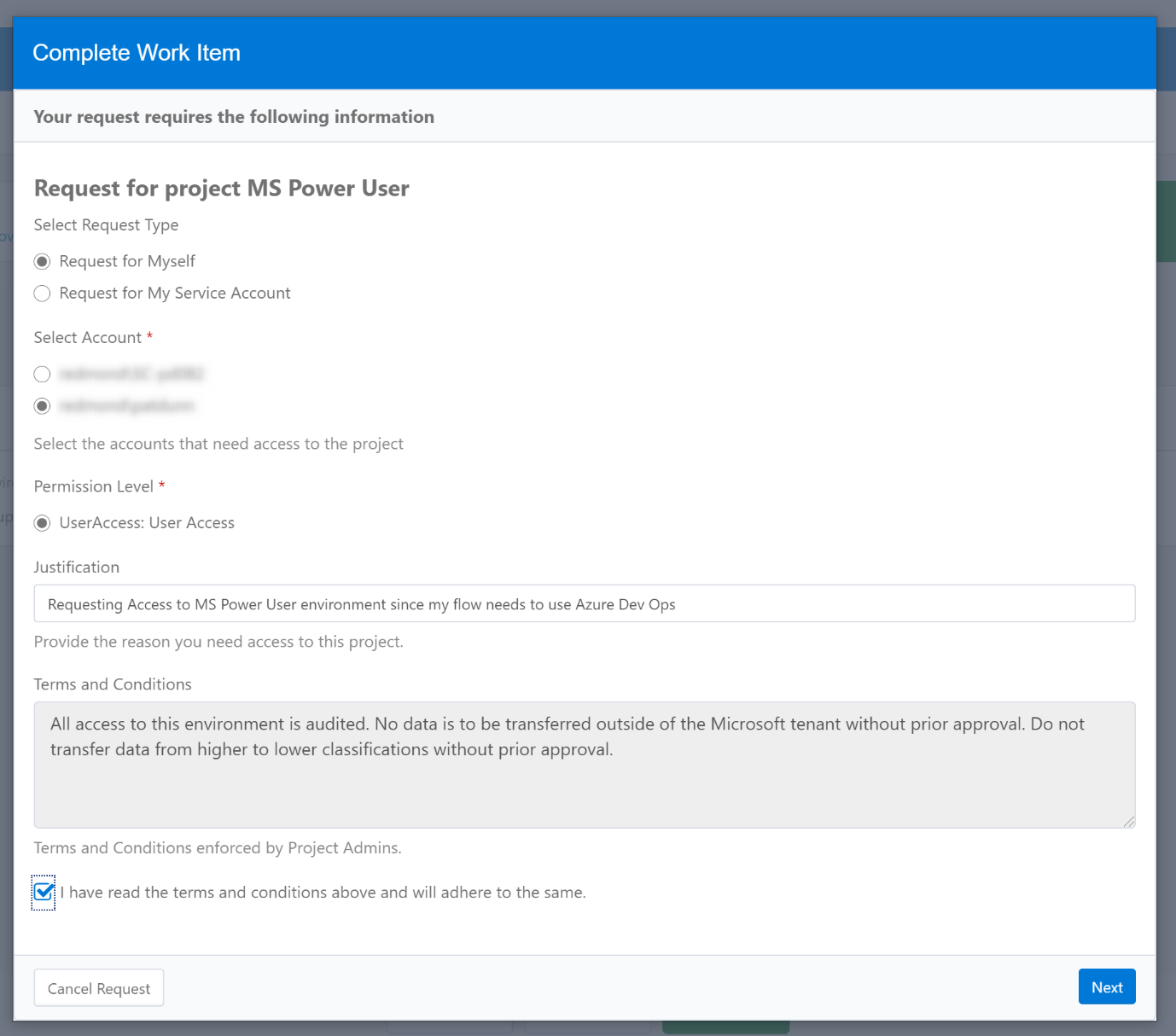
For this purpose we’ve created the Contoso Power User environment. This shared environment uses the **CONTOSO Low Policy** which enables many more connectors.

Some considerations for the Contoso Power User environment:

* Please review the **available connectors** in this environment to make sure it’s the right fit for your app and flow needs.
* Once you’ve gained access to the environment, you’ll have **Environment Maker** permissions. This will give you the permission to create new objects, like apps and flows, and some shared connectors. You will not, however, have the permission to grant Environment Maker permissions to others. Anyone who needs permission to create new objects will need to request Environment Maker permissions as well.
* Objects you’ve created can be shared with others, but please be careful to not overshare.

#### Gaining access to the Contoso Power User environment

1. Make sure your device is connected to corpnet
2. Go to https://<MSPowerUserRequestUrl>
3. If you are not already authenticated, then you may be presented with a search form. You have 2 options:
   1. Easiest option: Click the link above a second time to go directly to the request form
   2. Enter “Contoso Power User” in the text box then click the Search button to find the access project. Click on the checkmark to the left of the project, then Next, then Submit
4. Fill out the request form​  
   ​



**Select Request Type** : you can select a personal account or a service account here  
**Select Account**: If you have more than one account linked to your identity (like an Alt account), you can select it here  
**Permission Level**: Select UserAccess: User Access  
**Justification** (optional): Why access is being requested

1. Check the “I have read the terms and conditions above and will adhere to the same” checkbox and click Next.
2. Wait 1 – 2 business days. You can check your access by opening our Welcome app. Note: If you get an Access Denied error, please don’t request access. Just wait and try again later.

### **Contoso Pro Dev**

The Contoso Pro Dev environment is a shared environment intended to be used by experienced developers to build more complex applications and flows. More powerful connectors, like SQL Server, Azure Blob Storage, and Azure Functions are available for use.

For this purpose we’ve created the Contoso Pro Dev environment. This shared environment uses the **CONTOSO Medium Policy​** which enables many more connectors.

Some considerations for the Contoso Pro Dev environment:

* Please review the **available connectors** in this environment to make sure it’s the right fit for your app and flow needs.
* Once you’ve gained access to the environment, you’ll have **Environment Maker** permissions. This will give you the permission to create new objects, like apps and flows, and some shared connectors. You will not, however, have the permission to grant Environment Maker permissions to others. Anyone who needs permission to create new objects will need to request Environment Maker permissions as well.
* Although you can’t grant Environment Maker permissions to others, you can still grant Owner permissions on existing objects to others. Due to the increased risk of the allowed connectors in the Contoso Pro Dev environment, grant this permission only to users who also have gone through this same onboarding process.
* Objects you’ve created can be shared with others to use, but please be careful to not overshare. Be sure to read the section on **Object Sharing** for more information.

#### Gaining access to the Contoso Pro Dev environment

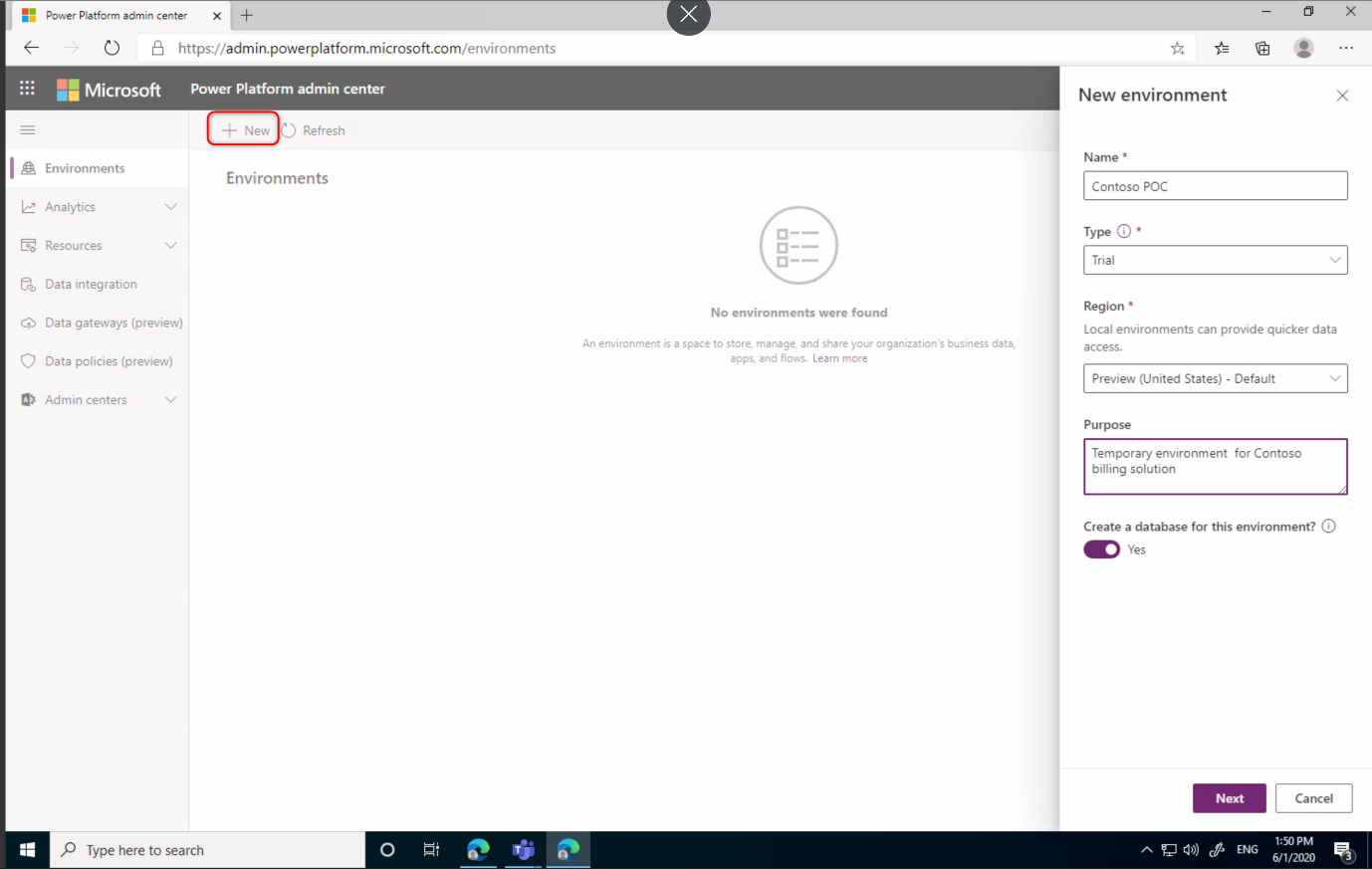
1. Make sure your device is connected to corpnet
2. Go to https://<MSProDevRequestUrl>
3. If you are not already authenticated, then you may be presented with a search form. You have 2 options:
   1. Easiest option: Click the link above a second time to go directly to the request form
   2. Enter “Contoso Pro Dev” in the text box then click the Search button to find the access project. Click on the checkmark to the left of the project, then Next, then Submit
4. Fill out the request form  
     
   **Select Request Type** : you can select a personal account or a service account here **Select Account**: If you have more than one account linked to your identity (like an Alt account), you can select it here  
   **Permission Level**: Select UserAccess: User Access  
   **Justification**: Why access is being requested. This will appear in the email sent to your manager
5. Check the “I have read the terms and conditions above and will adhere to the same” checkbox and click Next.
6. Your skip level manager will receive an email and will need to approve the request
7. Once approved, wait 1 – 2 business days. You can check your access by opening our Welcome app. Note: If you get an Access Denied error, please don’t request access. Just wait and try again later.

## Trial Environments

Trial environments are intended to support short-term testing needs where you have a legitimate business need to access data and resources in the Contoso tenant. Trial environments automatically expire after 30 days and are limited to one user.

In the Contoso tenant, trial environments are provisioned with the **CONTOSO Ultralow Policy**, limited to personal productivity connectors. This being the case, trial environments have limited usefulness. If you are using a trial environment to experiment with the Power Platform, consider creating a new demo tenant using the instructions elsewhere in this document.

If you still want to create a trial environment, follow these steps:

1. Go to <https://admin.powerplatform.microsoft.com/environments>
2. If prompted, sign in with your Microsoft credentials
3. Click New and fill out the New Environment form that appears on the right side of the screen:  
    

**Name**: enter a unique name for the environment  
**Type**: Select Trial. Although other environment types may appear in this list, only Trial will work  
**Region**: Select the region (data center) in which the environment will be created. This can be beneficial for performance. If you’d like to take advantage of Preview features and bug fixes, select Preview (United States) - Default

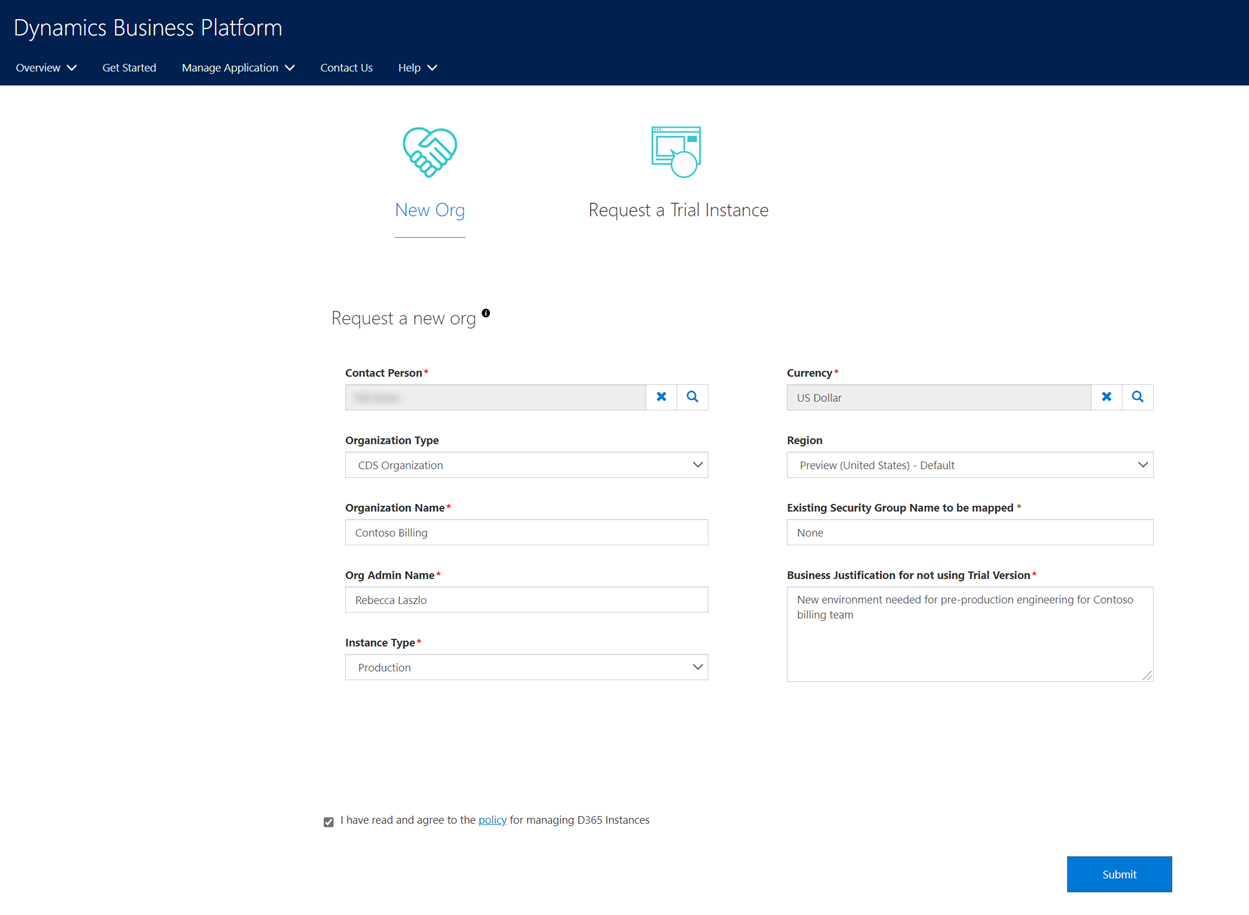
## Custom Environ​ments

While the shared environments in the Contoso tenant cover most use cases for applications, teams may benefit from creating a custom environment. See the **Purpose of Environments​** section for some common reasons why a team or organization may require a separate environment where you can exercise greater control.

Some considerations for custom environments:

* By default, a new environment will be provisioned with the **CONTOSO Ultralow Policy**. If more connectors are required, you can review the **pre-approved CONTOSO policies** below or request a **Custom Policy** with DSRE review. Please contact **Power Automate and Power Apps DLP** at https://<linkToForm>​ for more details.
* The requestor will be a System Administrator in the new environment. The administrator has full control to manage resources and user access. It will be your responsibility to manage access control wisely.
* Please familiarize yourself with the other available options before creating a custom environment since there is a cost to Microsoft for each environment. If you don’t need Contoso data, use a **demo environment**. If you do need Contoso data, look at the **shared environments** or a **trial environment** first.
* If an environment is no longer needed, delete it!
* CONTOSO is evaluating a cross charge for environments in the future to recover costs and encourage environment hygiene. Provision your environments sparingly.

To create a custom environment, please follow these steps:

1. Go to [https://dynamicsatmsft.microsoftcrmportals.com](https://dynamicsatmsft.microsoftcrmportals.com/)
2. On the top nav, click Get Started
3. Click on New Org
4. Fill out the New Org request form  
     
   **Contact Person:** The new org requestor  
   **Organization Type:** Unless you need Dynamics 365 modules, select CDS Organization  
   **Organization Name:** The name of the environment  
   **Org Admin Name:** This person will be granted the System Administrator role on the environment  
   **Instance Type:** Select Production unless you want a Sandbox environment (a pre-production environment that can easily be reset back to a blank environment)  
   **Currency:** Select the currency type used for the environment (i.e. US Dollar)  
   **Region:** Where the environment will be located. For US, you can select either standard or Preview (default)  
   **Existing Security Group Name to be mapped:** Use this only if want to limit the users that can be provisioned in the environment. Otherwise specify 'None'  
   **Business Justification:** Why is this environment needed?  
   ​
5. Select the ‘I have read and agree to the policy for managing D365 instances’ and click Submit

After submitting your request, you'll receive an email from Dynamics@contoso.com with your case number for tracking purposes. The SLA is 3 business days for provisioning the new org. For more information on the provisioning process, please read the **FAQ**.

Please note that the new environment will be pre-provisioned with the CONTOSO UltraLow policy (the same as Contoso Personal Productivity (contosodefault) ). Please see the top of this section for instructions on how to change the policy.

# Data Loss Prevention (DLP) Policies

A Data Loss Prevention (DLP) Policy is created by a tenant administrator as a way to protect information security in the tenant. A DLP policy allows an administrator to enforce which connectors are enabled for each environment.

At Contoso, DSRE has reviewed available connectors to analyze their risk. Several pre-approved policies have been created and available for our shared environments and can be enabled for custom environments. Those policies are **CONTOSO UltraLow**, [**CSO Low**](https://microsoft.sharepoint.com/teams/CSEOPowerApps/SitePages/CSEO%20Power%20Platform%20Wiki%20-%20Home.aspx#dlp_cseo_low), **CONTOSO Medium**, and **CONTOSO Medium Isolated.**​

New connectors are available periodically and DSRE will add those to our shared policies as appropriate. **Custom policies** are also available by request. If you would like a custom policy or would like a connector to be evaluated for an existing policy, please contact **Power Automate and Power Apps DLP** at https://<formtocontact>​​.

## CONTOSO UltraLo​w (Default Policy)

The CONTOSO UltraLow policy contains first party connectors that have been evaluated by DSRE and enabled as the default policy for the **Contoso Personal Productivity  (contosodefault)** and **Trial** environments. Any **custom environments** that are created will be configured with this policy by default, but can be changed once the environment is created.​

## CONTOSO Low (Contoso Power User)

The CONTOSO Low policy contains all the connectors of the CONTOSO UltraLow policy and adds several additional connectors that are useful for power users, like Azure AD, Kusto, and Power BI. Because these connectors expose more risk to Contoso data, makers must understand and attest to their proper usage before they are permitted to use this policy. This policy is enabled in the **Contoso Power User** shared environment.

​​​

## CONTOSO Medium (Contoso Pro Dev)

The CONTOSO Medium policy contains all the connectors of the CONTOSO UltraLow and CONTOSO Low polices and adds several connectors, like SQL Server and Azure Blob Storage, that can be used by more experienced developers to build more powerful applications.

Since these connectors pose a significant risk to loss of Contoso data if used incorrectly, makers must understand and attest to their pr​oper usage before they are permitted to use this policy, and a Principal-level manager must sign off on the risk. This policy is enabled in the **Contoso Pro Dev​** shared environment.​

## CONTOSO Medium​ - Isolated (Custom Environments)

The CONTOSO Medium - Isolated policy includes all connectors in the CONTOSO Medium policy a​nd adds the CDS connector. This policy can be applied to **custom environments**. Please contact **Power Automate and Power Apps DLP** at https://<formtosendrequest>​ for more information​.

## Comparing DLP Policies​

​ Here are the currently approved connectors and the policies in which they are enabled:

A screenshot of a cell phone

Description automatically generated

## Adding New Pre-Built C​onnectors​

​At the​ time of this writing, the Power Platform enables over [**325 connectors**](https://us.flow.microsoft.com/en-us/connectors/) to common services and this number grows constantly. ​As new connectors are added to the Power Platform, they are **not** automatically added to CONTOSO policies. If you wish to have a new connector reviewed, Please contact **Power Automate and Power Apps DLP** at https://<url>​ to review the new connector. It will be evaluated for its risk to Microsoft and added to the appropriate policies.

## Adding Custom Connectors

With the use of [Custom Connectors​](https://docs.microsoft.com/en-us/connectors/custom-connectors/), your Power Apps and Power Automate Flows can communicate with many more services, like a custom API built by a service owner. Custom connectors need to be added to a DLP policy to work with your apps and flows. Generally these would be added to a custom policy in a custom environment, but in special cases where there is a broad need for the connector, we can add it to one of our shared policies like CONTOSO Low. Please work with **Power Automate and Power Apps DLP** at https://<url> to review your custom connector and add it to the appropriate policy.

## The SAMPLE Connector

The SAMPLE connector is a community-built custom connector hosted in the Contoso Personal Productivity environment, and will eventually be deprecated. The DLP team has approved its use in Contoso Power User and Contoso Pro Dev, but first it must be re-written and go through a security review. The governance team is looking at taking ownership of this connector and doing the work necessary (it’s in the backlog). Currently, we do not have a time commitment. Until this work is complete, we do not have a good solution for integrating with SAMPLE outside of Contoso Personal Productivity . For now, this connector is enabled in the CONTOSO UltraLow policy and you can use it for new or existing solutions.

## Custom Policies

The CONTOSO policies have been created by DSRE with connectors suitable for each environment. If you create a Custom Environment, it will default to CONTOSO UltraLow. However, you can contact **Power Automate and Power Apps DLP** at https://<url>​ to change the policy of that environment to CONTOSO Low on request. CONTOSO Medium or CONTOSO Medium Isolated may also be requested, but will require management approval.

In some cases, you may require a connector not in one of the pre-approved DLP policies. For example, you might need to enable a 3rd party connector. Please contact **Power Automate and Power Apps DLP** at https://<url>​ for assistance.

​

# ​Environment Roles and Object Sharing

To safely share in the Power Platform Contoso tenant, it’s important to understand how permissions and sharing work. Failure to share your objects correctly can put Contoso data at risk.

Environment permissions are handled through *Environment Roles* and sharing is handled through *Object Permissions*.

## Environment Roles

At the environment level, there are two roles that can be assigned to users in the Contoso tenant for non-CDS environments, and several more for environments with a CDS database.

### **Environment Maker**

For all shared environments (Contoso Personal Productivity , Contoso Power User, and Contoso Pro Dev), only the **Environment Maker** role will be assigned. **Environment Maker** allows anyone with that privilege to create new apps, flows, and shared connections. When the **Environment Maker** creates an object, like an app or a flow, they will be the owner of the object and can share the object with others.

Notes for the **Environment Maker** role:

* The **Environment Maker** cannot grant that role to others. Each user who needs to get **Environment Maker** permissions will need to request that role.
* An **Environment Maker** cannot see the objects that other **Environment Makers** have created in the same environment.

### **System Administrator**

If you create a trial or custom environment, you will be the **System Administrator** for that environment. The **System Administrator** has full permissions on the environment, including the ability to rename or delete the environment. The **System Administrator** can also grant roles, like System Administrator or Environment Maker, to others in the tenant.

Notes for the **System Administrator** role:

* The **System Administrator** can see, modify, and delete all objects in the environment
* Due to the increased risk of this role, grant it sparingly

## Other Environment Roles

If you create a CDS or Dynamics 365 environment then there will be several other built in roles, as well as the ability to create custom roles. To learn more, visit <https://docs.microsoft.com/en-us/power-platform/admin/environments-administration>

## Service Accounts

A service (or system) account is a better way to access data and services with less risk to Contoso data than a user account. For more information, please see https://<url> (corpnet access required). A service account can be used to create objects in environments that, when viewed by other users, are linked to an identity that isn't a user. For example, the ApplicationName applications are published by the CONTOSO Power Apps account to distinguish them from citizen-developed apps, shield individual developers from user requests, and allow for team members to join or depart the team without having to change credentials.

Service accounts are also very useful for connections in Power Automate flows. For example, if you use the credentials of a real person to access the Office 365 Outlook connector then share that flow with Owner permissions to others, the other owners will be able to impersonate that user for Office 365 Outlook calls. They can read, write, and delete mail, contacts, calendars, and more.

### Getting a Service Account

To get a service account, follow these steps:

1. Connect to corpnet, either on-premise or through a VPN
2. Navigate to https://<url> and, if prompted, sign in with your corporate credentials
3. Click on the ACTIVE SERVICE ACCOUNTS section
4. Click on the + CREATE NEW ACCOUNT button
5. Fill out the form fields as required and wait for the confirmation mail that the account has been provisioned.

### Licensing a Service Account

But service accounts are not automatically provisioned for Power Platform licenses in the Contoso tenant and cannot be added to environment roles until they have a license. To get a license, do the following:

1. Go to https://<filloutaform> and sign in with your Microsoft credentials
2. Fill out the form as follows:
   1. **Category of issue**: Application & Service
   2. ​​**Select the impacted Application**: User Account
   3. **Short description**: “Please grant the Microsoft Power Apps Plan 2 Trial license to the account {account alias}@microsoft.com”
   4. **Other fields:** fill out as desired
3. Submit the form
4. You’ll receive an acknowledgement of the incident followed by a confirmation the ticket has been resolved
5. To validate the license, do the following
   1. Navigate to <url>
   2. Search for your service account and click on it in the search results
   3. On the left nav, click on Licenses
   4. Validate that the account has the **Microsoft Power Apps Plan 2 Trial** license
6. Once the license appears, go to <https://admin.powerplatform.microsoft.com/environments>, search for the environment, and select it
7. Click on Settings on the top N\nav
8. In the Settings screen, click on Users and Permissions to expand it, then click on Users
9. Click the Add User button on the top nav, search for your account, then click Add
10. You will receive a confirmation message that the user has been added but no role has been assigned. Click the button to go to the Dynamics interface to add them to the desired role

### ​​Working as a Service Account

Your service account will have a user name and password, but will require Multi-Factor Authentication (MFA) in order to sign into www.powerapps.com or flow.microsoft.com. For service accounts, this means that the sign-in will need to happen from a known Microsoft network. Unfortunately, a VPN connection is insufficient. You'll need to do one of the following:

1. ​Sign in from an on-premise location, like wi-fi access in a Microsoft building  
     
   - or -
2. Establish a Remote Desktop session to a "Jump Box", which is a machine operating inside corpnet, either on-premise or an IaaS VM  
     
   - or -
3. Sign up for a Windows Virtual Desktop (WVD). This creates a virtual machine that you can use inside Microsoft corpnet. Follow the instructions at **<url>** for more information.

Once you've successfully logged into the Power Platform as the service account, you'll be able to create objects if you are an Environment Maker and you'll be able to add the service account's connections to your flows. You can share the flow with owner permissions to other trusted users and they'll be able to use those connections in the flow. Be sure to scrub any connections belonging to a real user in a shared flow, and use only the service account connections.

### Emailing with a service account

You do not need a password for your service account if its mailbox only (you can ignore the licencing and working with service accounts above - if its mailbox only).

To send an email with the Power Platform, make sure you are using the Office 365 Outlook connector, select advanced, and enter the service account in the "send-as" box.

Make sure in <url>, you have granted your account (or the account of the Outlook connection owner) the "send-as" permissions. Full Permissions is different, and will not grant the required rights. If you run into issues check you can "send-as" this service account in the Outlook app or OWA.

To get permission to send email externally - you need to be using a service account. Once you have one, you can request allow-listing via the **Power Automate and Power Apps DLP**team at <url>  
​

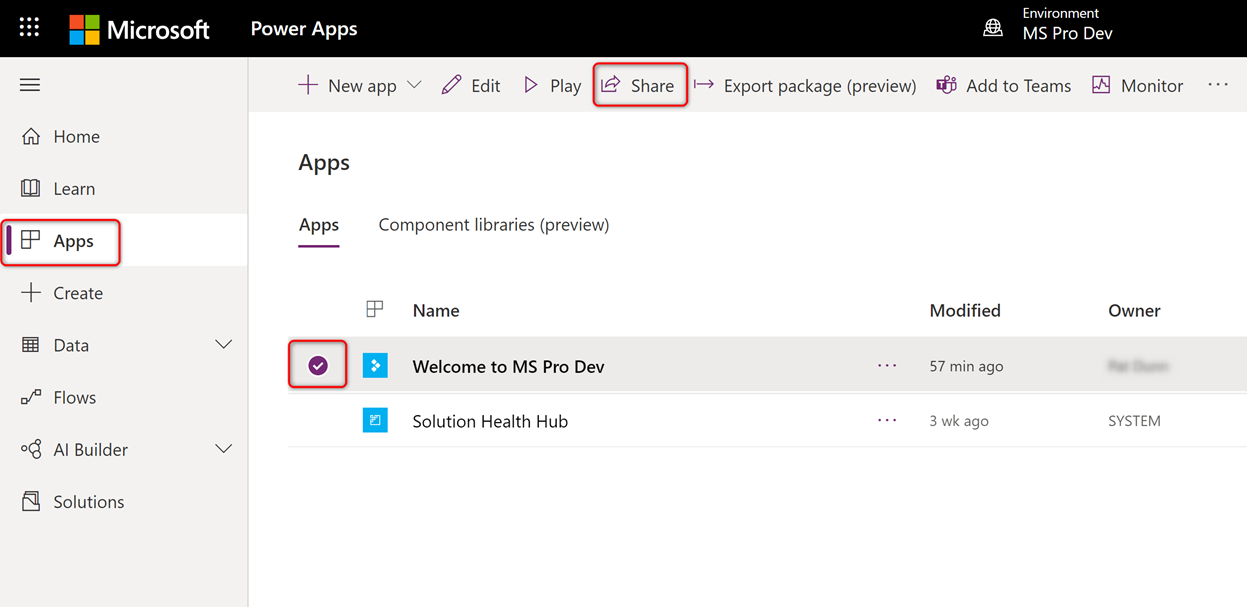
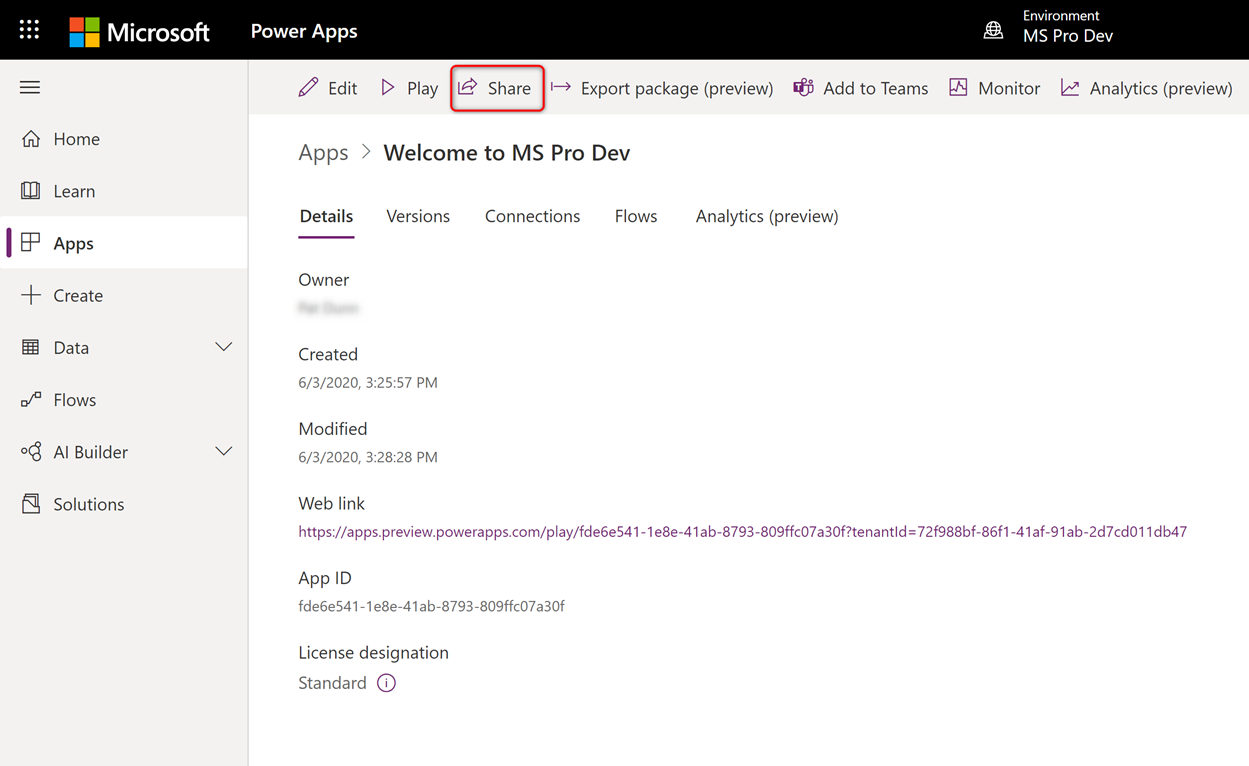
## Object Sharing

It’s easy to share your apps, flows, and connections in the Contoso tenant. When you share your objects, you increase the risk that the object will be overshared and Contoso data could be compromised. To avoid this risk, please adhere to the following guidelines:

* Adhere to the [Principle of Least Privilege](https://en.wikipedia.org/wiki/Principle_of_least_privilege). Only share your objects with the people that need to see the object, and only grant them the minimum permissions needed to access the object.
* Avoid granting Owner permissions to someone who is not already in the **Environment Maker** role.
* Never share with the ‘Everyone in Contoso’ group, since this includes guest access. For example, if someone works with an external vendor and grants them access to a SharePoint document, they are considered a guest in the Contoso tenant. If you then grant access to your object to ‘Everyone in Contoso’, that same user will be able to access your object and potentially compromise Contoso data.  
    
  Wherever possible, share with a group instead of individuals. The Power Platform supports AAD groups and Office groups. Managing access then becomes much easier as you only need modify the group instead of every app, flow, connector, etc. Sometimes you might need to add an individual while their group permissions are replicating, but this should be temporary.
* Review sharing permissions frequently. We recommend that you review your object permissions at least every 90 days

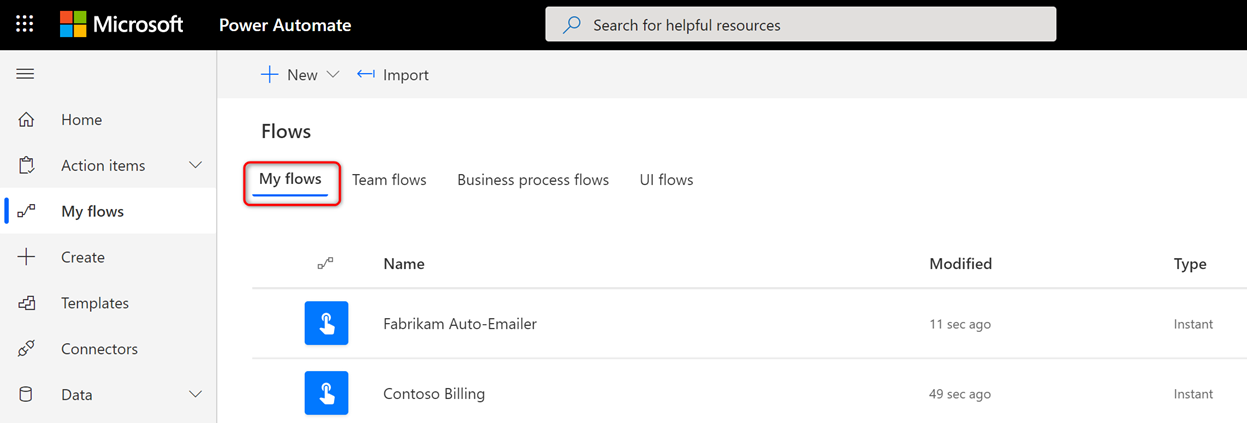
### **Power App Sharing**

Once a Power App has been published, it can be shared with individuals or groups. Optionally you can grant Owner permissions to the app, which allows that user or group to edit the app as well. There are many ways to do this:

1. When you Save a canvas Power App, you’ll be prompted first to Publish, then to share the app
2. In the apps tab of powerapps.com, you can select an app, then share it. You can also access the Share feature by clicking on the ellipsis  
   
3. From the App Details page, select the Share button  
   

### **Power Automate Flow Sharing**

Power Automate Flows, by default, are private. Only the owner of the Flow will be able to see and modify the Flow. You can tell if you are the only owner of a Flow as it will appear in the My Flows tab.

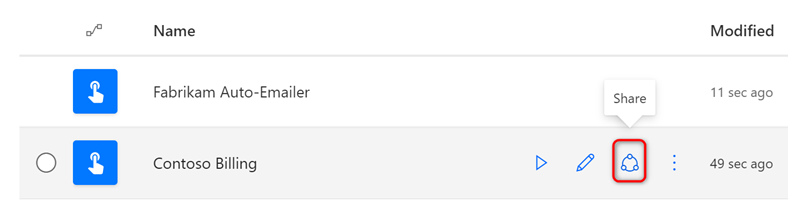


Flows can be shared with Owner or Run-Only permissions. Be aware that if you share ownership of a Flow, the other owners will be able to use any connection that you’ve added to the Flow. They will be able to impersonate you in access to services, such as accessing your inbox. **If you have more than one owner of a flow, use only service account credentials for your connections.**

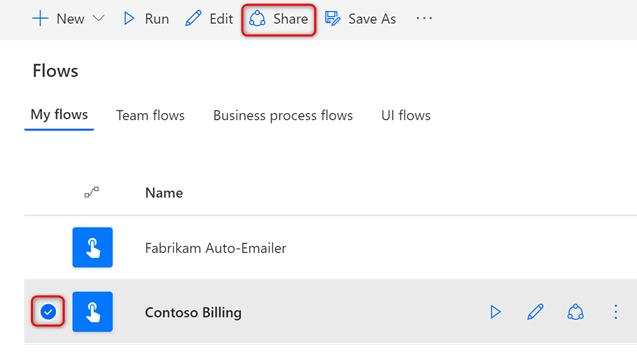
#### Sharing Flow Ownership

It's good practice to have more than one owner of a Power Automate Flow in the event that someone leaves the company or is unavailable when critical edits need to be made. There are many ways to share ownership of a Power Automate flow, including:​

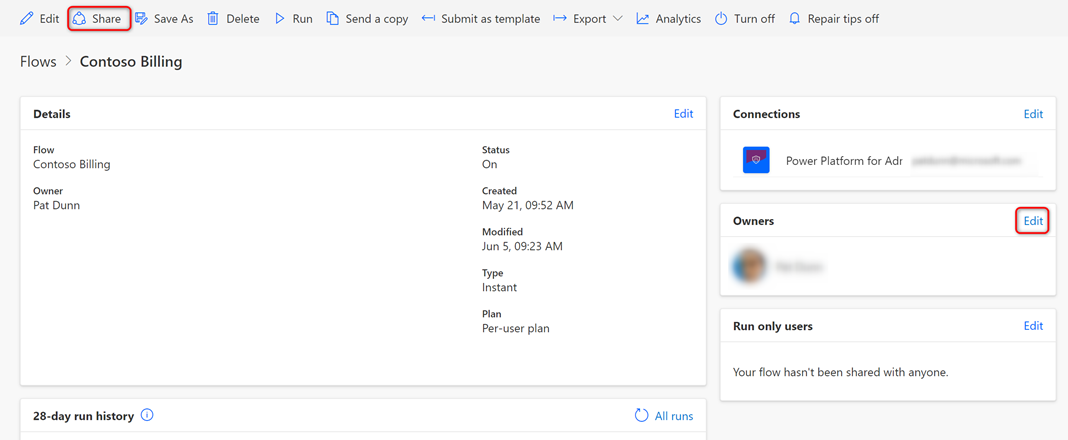
1. Hover over a Flow and click on the Share Icon



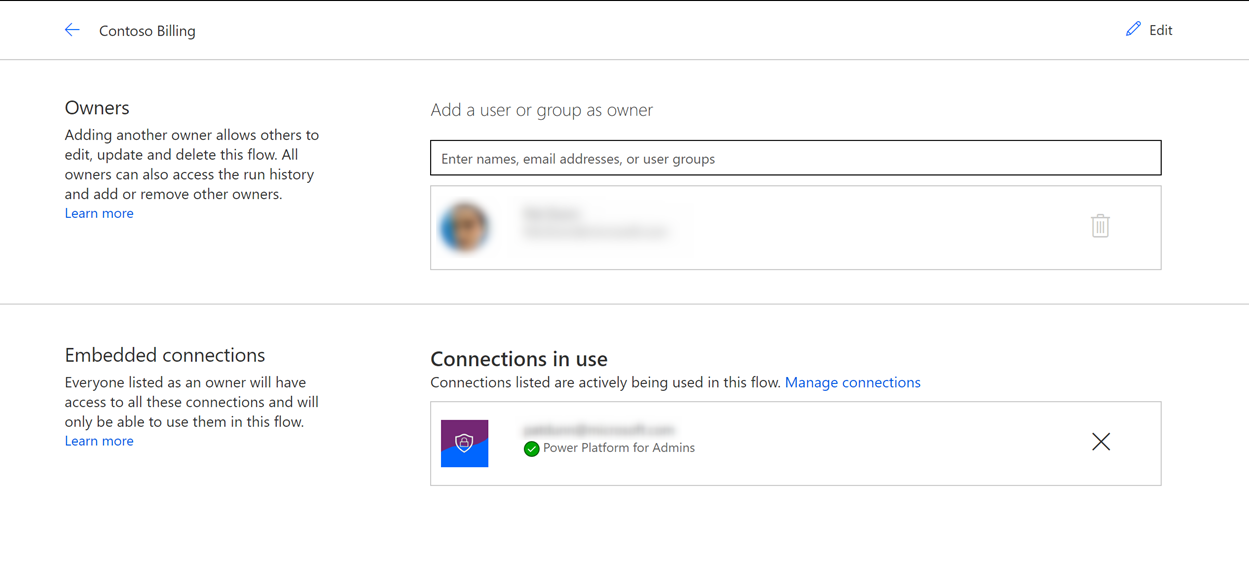
1. Select a Flow and click the Share button on the top nav



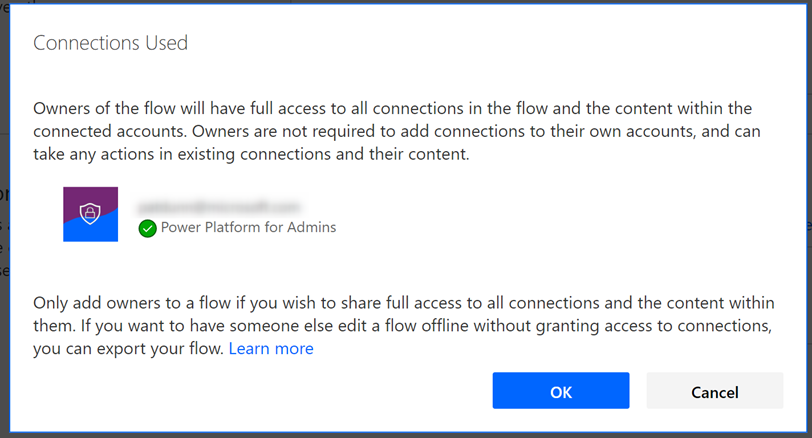
1. Select a Flow to go to its Details page and click Share on the top nav or Edit in the Owners box



Once you’ve reached the sharing screen, add other owners of the Flow



Once you’ve selected another owner, you will see a warning that you will share your connections with them



Click OK and the Flow will be shared with the selected user(s). The Flow will now appear in the Team Flows tab. Anytime the Flow is modified, all owners will receive a notification mail.

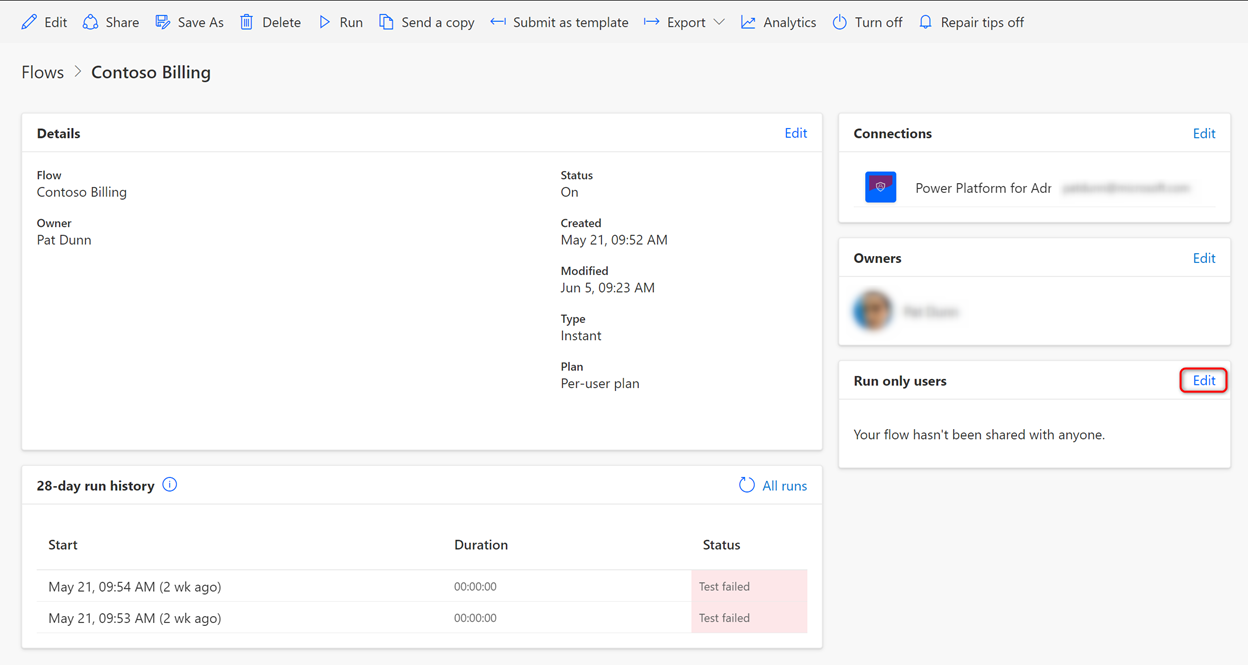
Tips

* DON’T share a flow that uses your own signed-in connections for services that extend your permissions to others. For example, if the Flow uses O365 Outlook, do not share your signed-in connection as other owners will have **FULL** access to your Exchange inbox.
* DO share a Flow with more than one person where it is not just for personal use. That way the Flow can be edited if you leave the company or are unavailable.
* DO share ownership of a Flow only with other users that are entrusted to work on behalf of the signed-in connections used in that Flow.
* DO share ownership of a Flow with a security group rather than with other individuals
* DO use service accounts or service principals rather than your domain account for any signed in connections in a shared Flow.

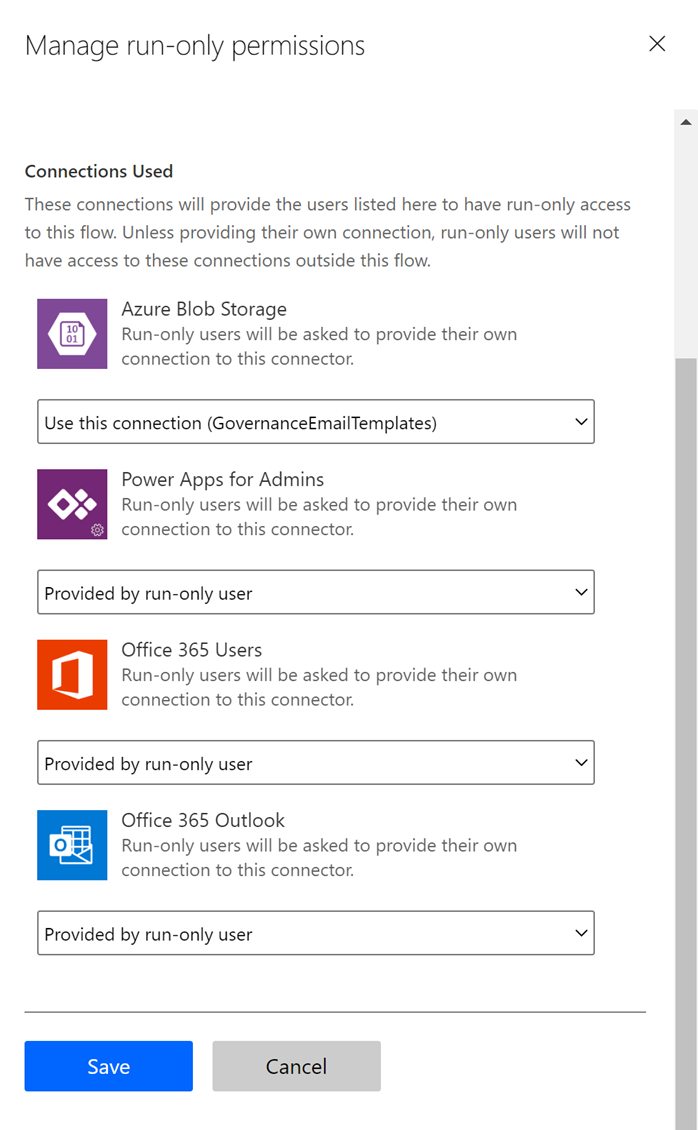
#### Sharing Flow Run-Only Permissions

If you are an owner of a Flow, you can grant Run Only permissions to others. To do this, follow these steps:

1. Find the Run only users widget at the right bottom of the screen and click on Edit



1. Select the users with whom the Power Automate Flow will be shared
2. Specify which connection ​should be used for each connector used in the Flow.



Select **Use this connection (connection name)** if you want to use the credentials that you specified when you created the connection. This can be useful in some cases, like when you have a service account that will access a service on behalf of the user.  
Select **Provided by run-only user** if you want the user to be prompted to sign in the first time they access the Flow. This can be useful where you need the user to use their own credentials, like when sending an email from their own account or accessing a site with their own credentials.

1. Press Save and the Run-only users will receive a notification mail with instructions on how to run your Flow.

Run-Only access has different risks than Owner access. With Owner access, you are trusting other owners with the signed-in credentials that you have added to a connection. With Run-Only permissions, the end user is trusting you, the owner of the Flow, to use their credentials safely.

### **Shared Connections**

A Connection is an instance of a Connector, where credentials have already been entered and the connection is signed-in. When you create a canvas app, you can add a connector like SharePoint, and the user will be prompted to sign in to create their own private connection the first time they launch the app.

But you can also create **Shared Connections** for some (but not all) **Connectors**. For example, you can create an Azure Blob Storage connection based off the Azure Blob Storage connector, supplying the path and user credentials for the Azure blob. This connection can then be shared by other users so that when they launch an app using that connection it’s already signed in.

This is very useful for when you have a specific account that will access a resource, but it can also be very dangerous for two reasons:

1. If someone has Environment Maker permissions in the same environment, they will be able to add a connection you’ve shared with them to their own apps or Flows in that environment. For an extreme example, if you have a shared SQL Server connection in the Default environment and you’ve shared that connection with Everyone at Microsoft, then anyone in the company can create a new app or Flow, add that SQL connection to it, and utilize the full permissions of that connector.
2. ​Even if someone doesn’t have Environment Maker permissions, a moderately skilled hacker can call the connection directly with an HTTP request and utilize the full permissions of that connection.

Tips:

* DO try to use Connectors rather than Shared Connections wherever possible. This will force the user to create their own private connection when they launch the app or Flow the first time.
* DO use service accounts for your Shared Connections whenever you can. That way other users aren’t impersonating a real domain account as they access resources.
* DO put your signed-in connections behind a Flow. To do this, don’t share the connection with anyone other than the makers of a Flow. Then share the Flow with Run-Only permissions to your end users. They won’t be able to call that connection directly, they can only call it via the Flow (which will control how that connection can be used).
* ​DON’T use a shared connection when a private connection can do the job. For example, the SQL connector allows both SQL Auth (shared connection) and AAD Auth (an individual connection). Use AAD Auth.

# Moving objects between envir​onments

Your apps, flows, connections, and other objects are contained in an environment. If you need to move your objects from one environment to another, like moving an app and its flows from Contoso Personal Productivity (default) to Contoso Power User, there are a number of ways this can be done.

## Moving a Power Platform solution

​Advanced users can create a Power Platform solution. A solution is a container for apps, flows, connections, CDS elements, and more. It's a great way to manage more complex applications where Application Lifecycle Management (ALM) is required, like developing in a pre-production environment and deploying the solution to production. It's also a handy way to migrate your solution from one environment to another. You can learn more by reading [Evan Chaki's announcement​](https://powerapps.microsoft.com/en-us/blog/solutions-in-powerapps/). Just be sure to export your solution as an Unmanaged Solution to the new environment.

## Moving a Power Apps canvas app

There are many ways to move a canvas app from one environment to another.

### **Saving the file locally**

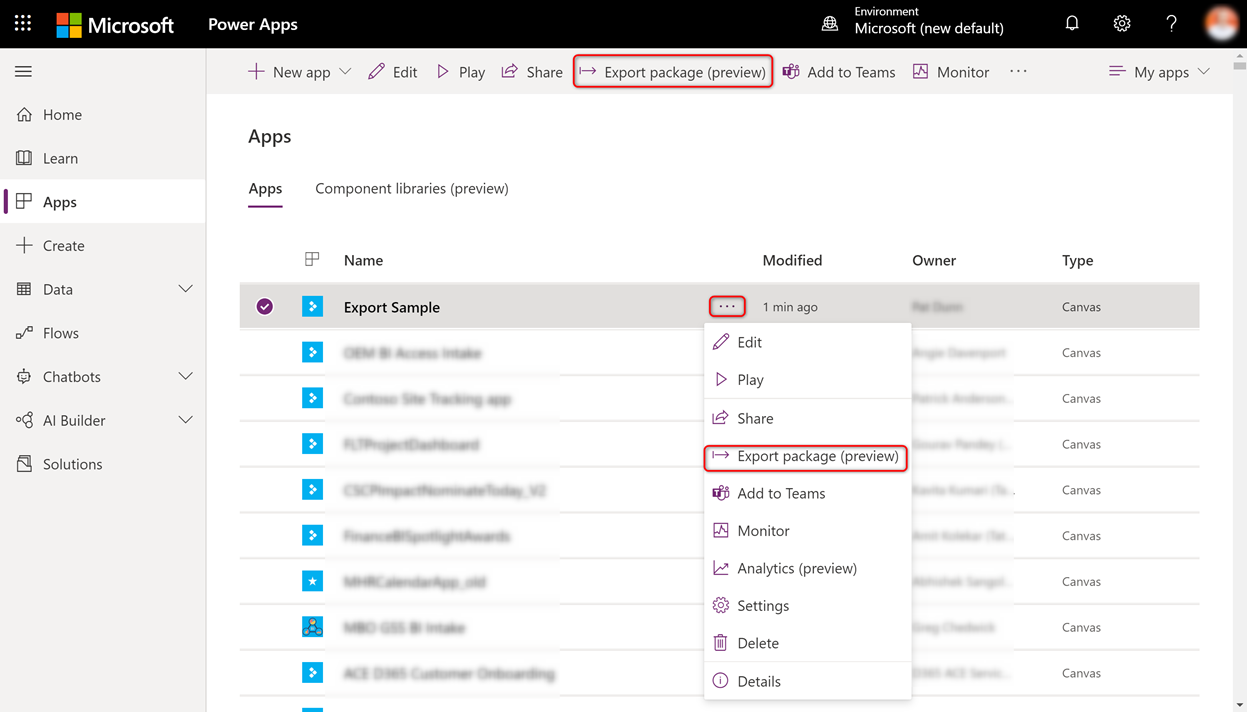
The simplest way to move your canvas app is to save it to your local computer from the Power Apps editor. That will create a \*.msapp file that can opened in another environment. The problem with this approach is that all connections will be broken – you will need to edit the app in the new environment, re-adding any connections manually in the editor. This approach isn’t recommended.

### **​**Using the Export package feature

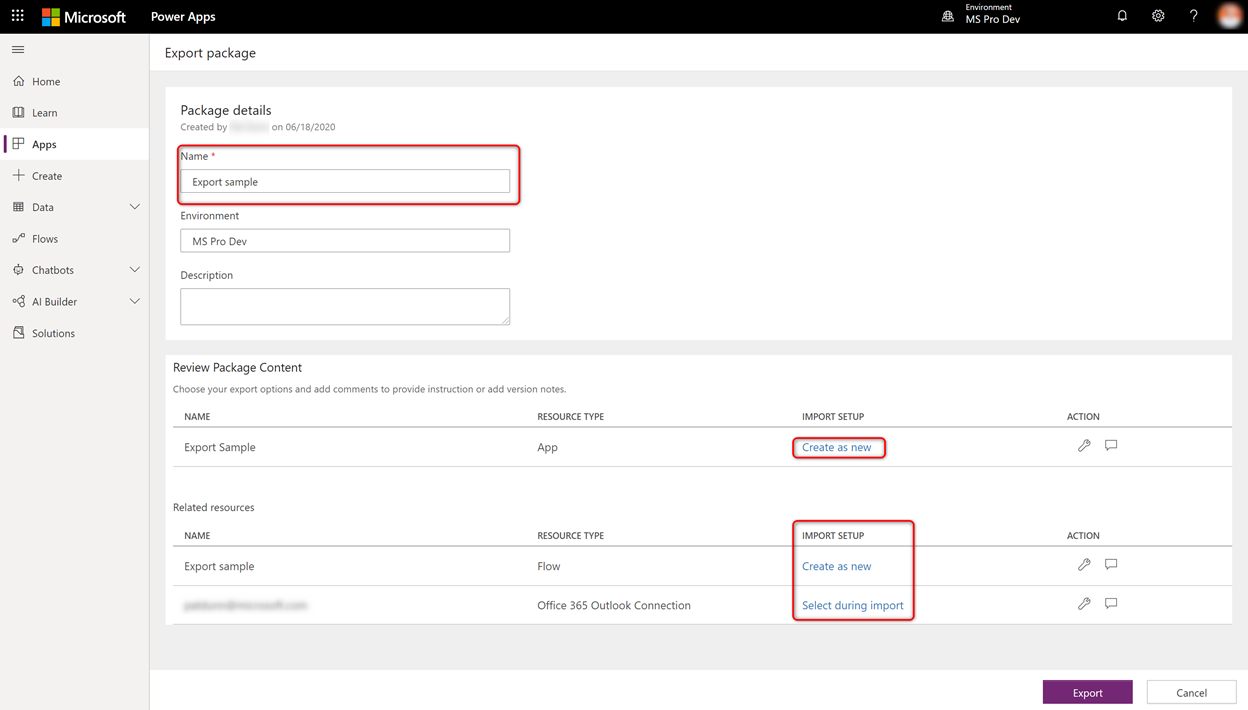
A much better way of moving a canvas app is with the Export package feature. This feature creates a package that the Power Platform can import into the target environment, letting you remap your connections and flows and merging CDS elements, like custom entities and option sets, during the process.

​To use this feature, follow these steps:

1. Sign into [https://powerapps.microsoft.com](https://powerapps.microsoft.com/) with your corporate credentials
2. Locate the app that you wish to migrate
3. Click to the left of the app to select it, then press the Export package (preview) button on the top nav or click on the ellipsis to the right of the app and select Export package (preview).​

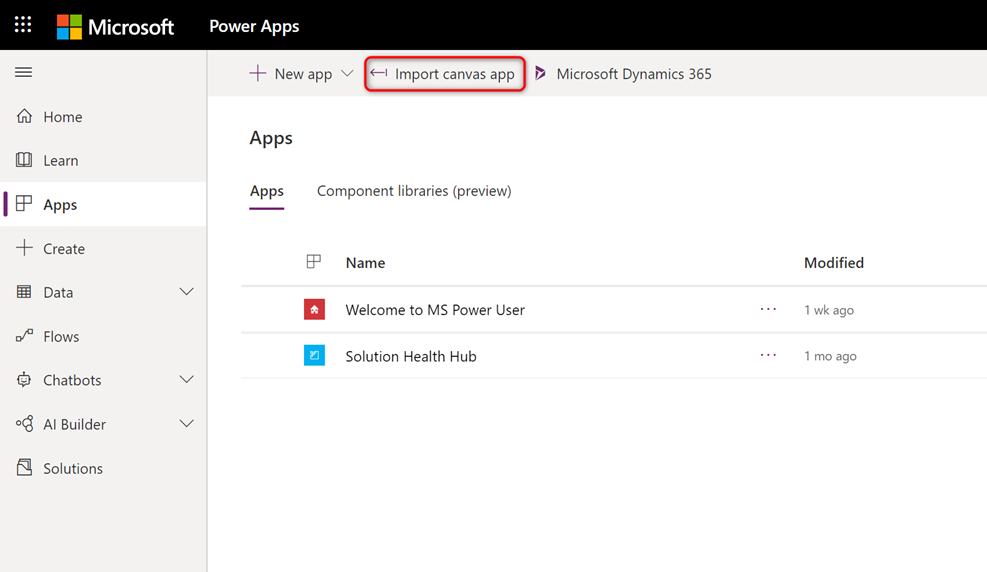


1. ​​​​On the Export package screen, fill in the form​

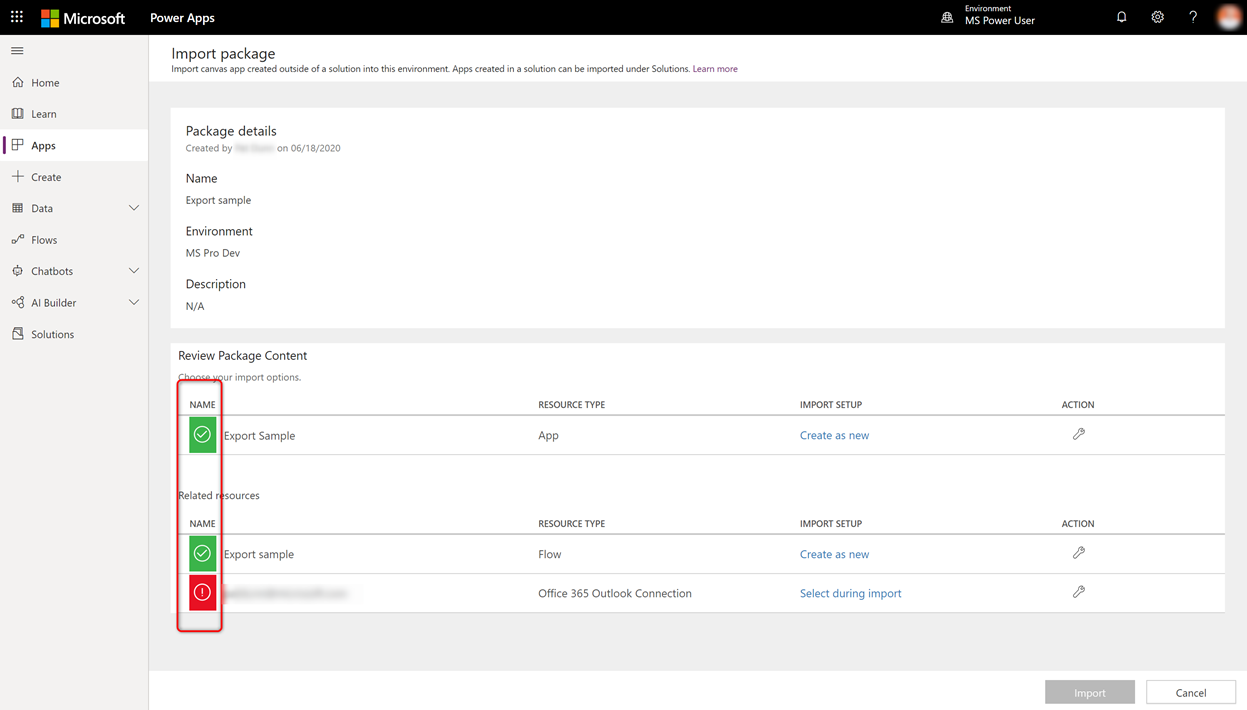


**Name** – this is the name of the package, not necessarily the app. It will be used for the filename  
**IMPORT SETUP** *(app)* – select Update if you are replacing an existing app, otherwise choose Create as new  
**IMPORT SETUP** *(Related resources)* – Available options will change depending upon the type of the resource. Connections will have to be selected during import, flows can be created as new or updated, and CDS resources will have other options.

1. Press the Export button and a zip file will be downloaded to your computer. This file will be saved to your downloads folder with the name you specified above and the date and UTC time of the download.
2. Navigate to the target environment. If the app relies on any shared connections (e.g. SQL Server), or a custom connector, then those objects will need to be manually created here before you can import the app.



1. Navigate to the Apps page and select Import canvas app from the top nav
2. On the Import package screen, click on the Upload button to locate the app package you saved in the previous step, then press OK
3. The package will load and you will need to fix any resources with a red exclamation mark before the file can be imported



1. Resolve all issues in the IMPORT SETUP column and press the Import button.
2. When the import is complete click the Open app link on the confirmation page to test your app before you share it.

A screenshot of a social media post

Description automatically generated

**Note** – When launching your application, you might receive this error:

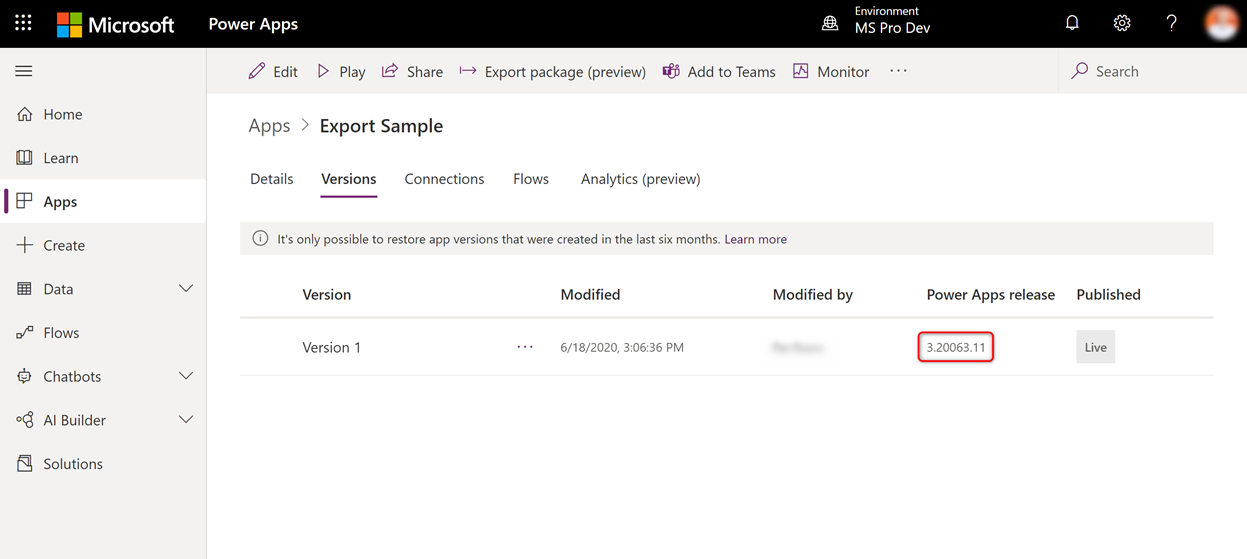
“Error opening file. The app you are trying to open was saved with a newer version of Power Apps and cannot be opened with the current version of Power Apps”

A screenshot of a cell phone

Description automatically generated

This error can occur if you export from a Preview environment like Microsoft (default). Apps that are created in Preview environments are built with a newer build of the Power Platform than a regular Production environment like Contoso Power User or Contoso Pro Dev.

 To check if this is the case, go to the details page of the newly imported canvas app, click on Versions, and look at the Power Apps release column. Compare that with the version number of a newly saved app in the same environment.



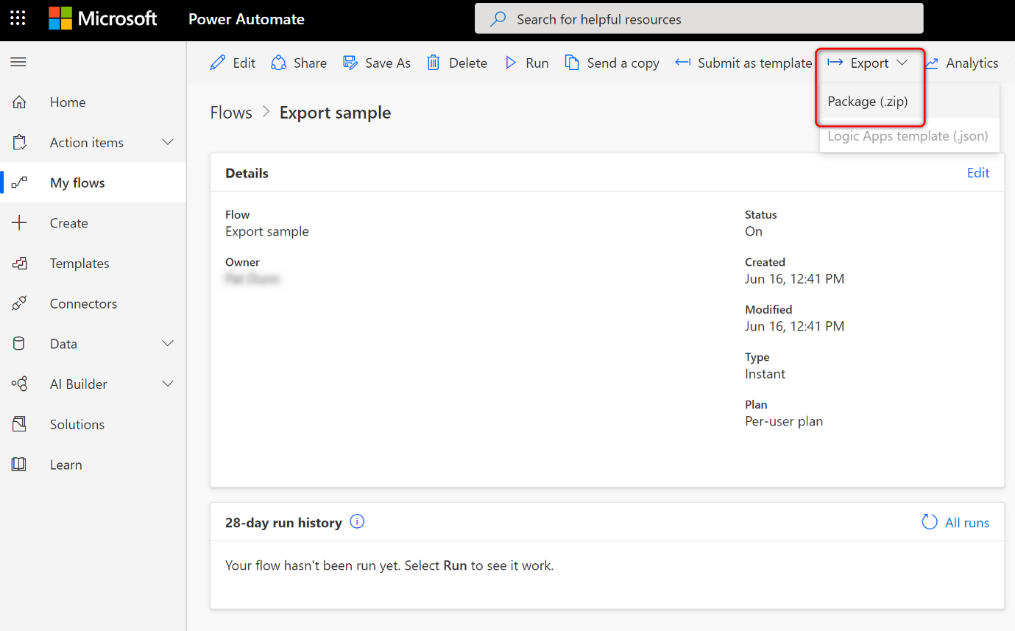
​You will need to wait until the Power Apps release number in the target environment is same or greater than the source environment. Typically this takes about a week, so plan ahead.

## ​Export​ing a Power Automate Flow to another environment

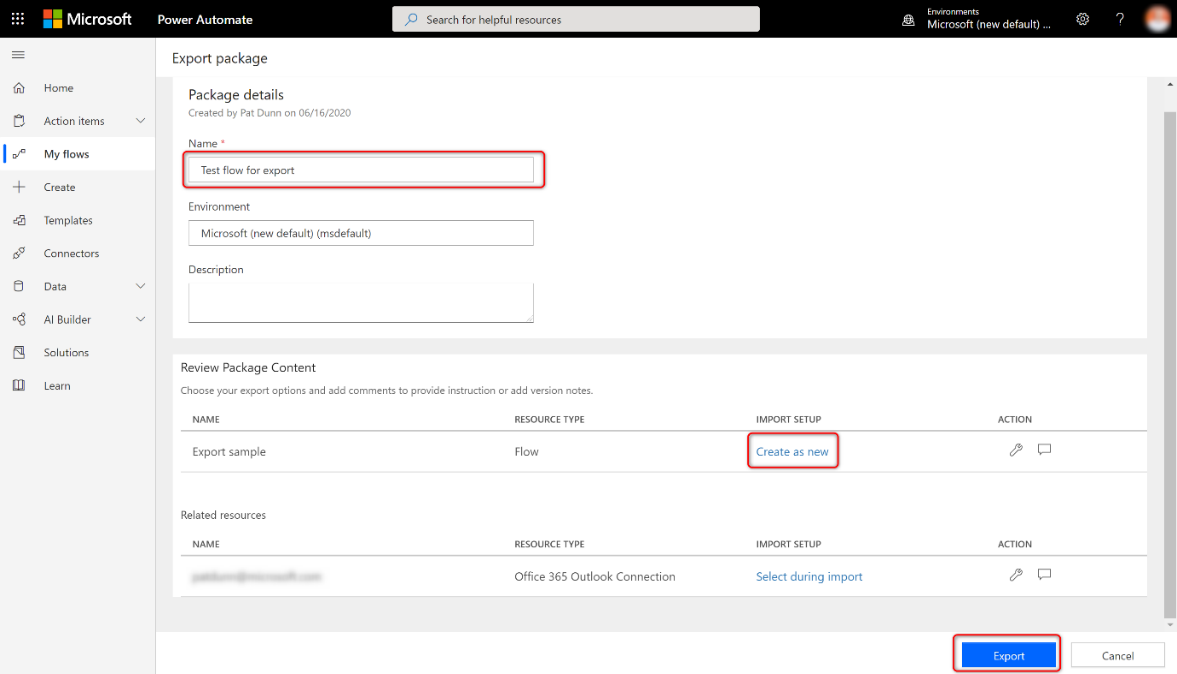
Just as with a Power App, there are a number of ways to move a Power Automate flow between environments. The simplest way is to export the flow as a package, then import that flow in another environment. To do this, follow these steps.

1. ​Navigate to [https://flow.microsoft.com](https://flow.microsoft.com/) and sign in with your MS credentials. **Note:**these steps only work from flow.microsoft.com, not from powerapps.com​
2. Select the environment where your flow is located from the environments list on the top nav
3. Click on My Flows on the left nav
4. Locate the flow you wish to export and do one of the following:
   * ​​Hover over the ellipsis and select Export…Package (.zip)  
     A screenshot of a social media post

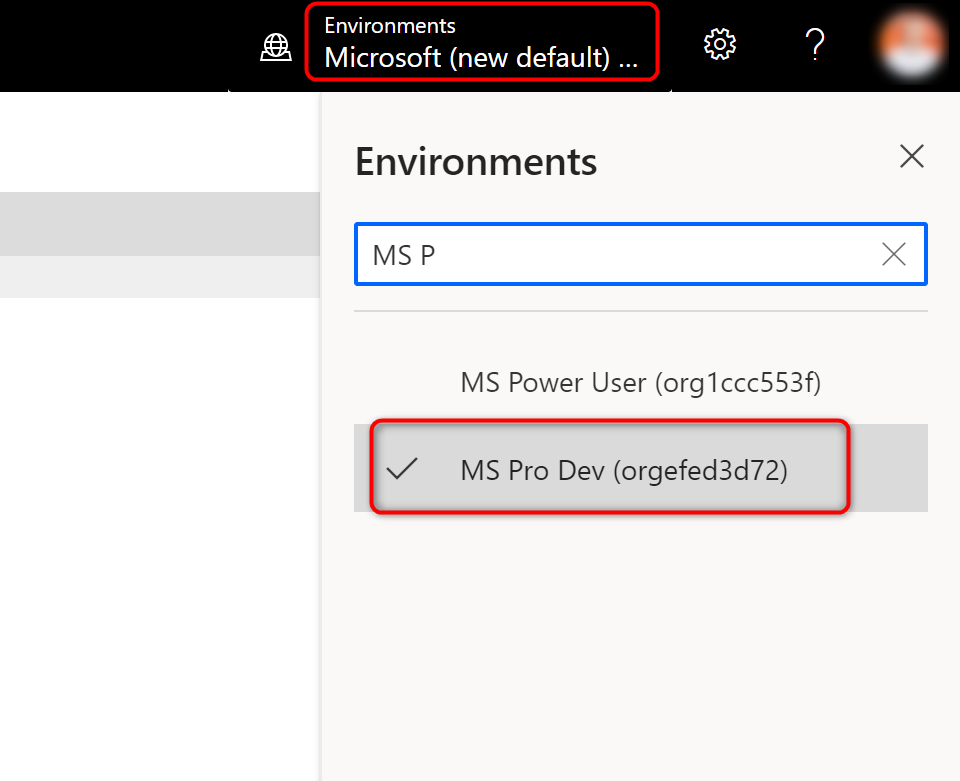
     Description automatically generated
   * Or click on the flow to go to the Details screen, then select Export…Package (.zip) from the top nav

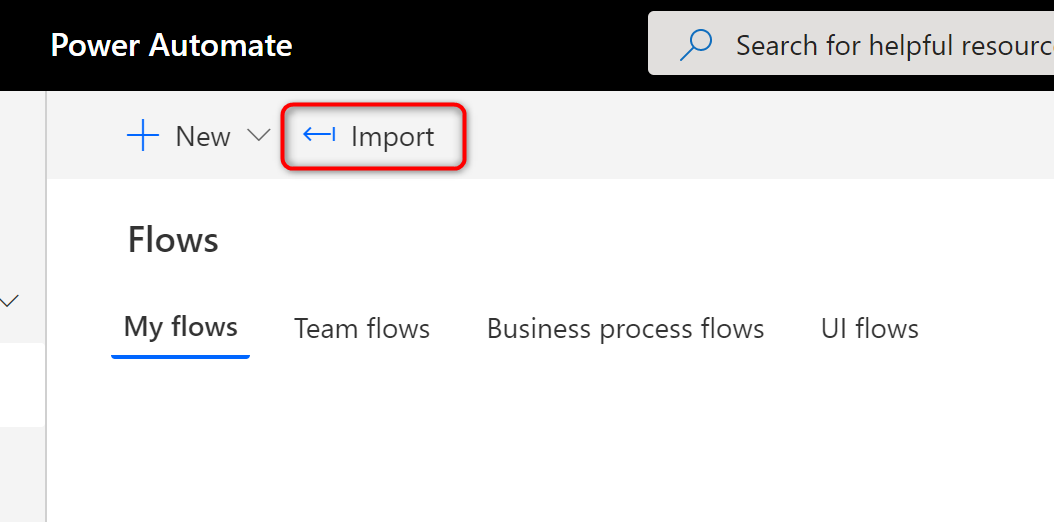


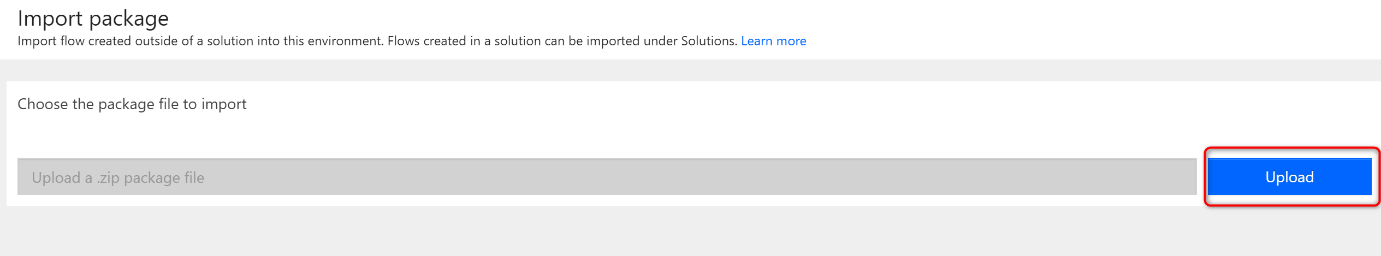
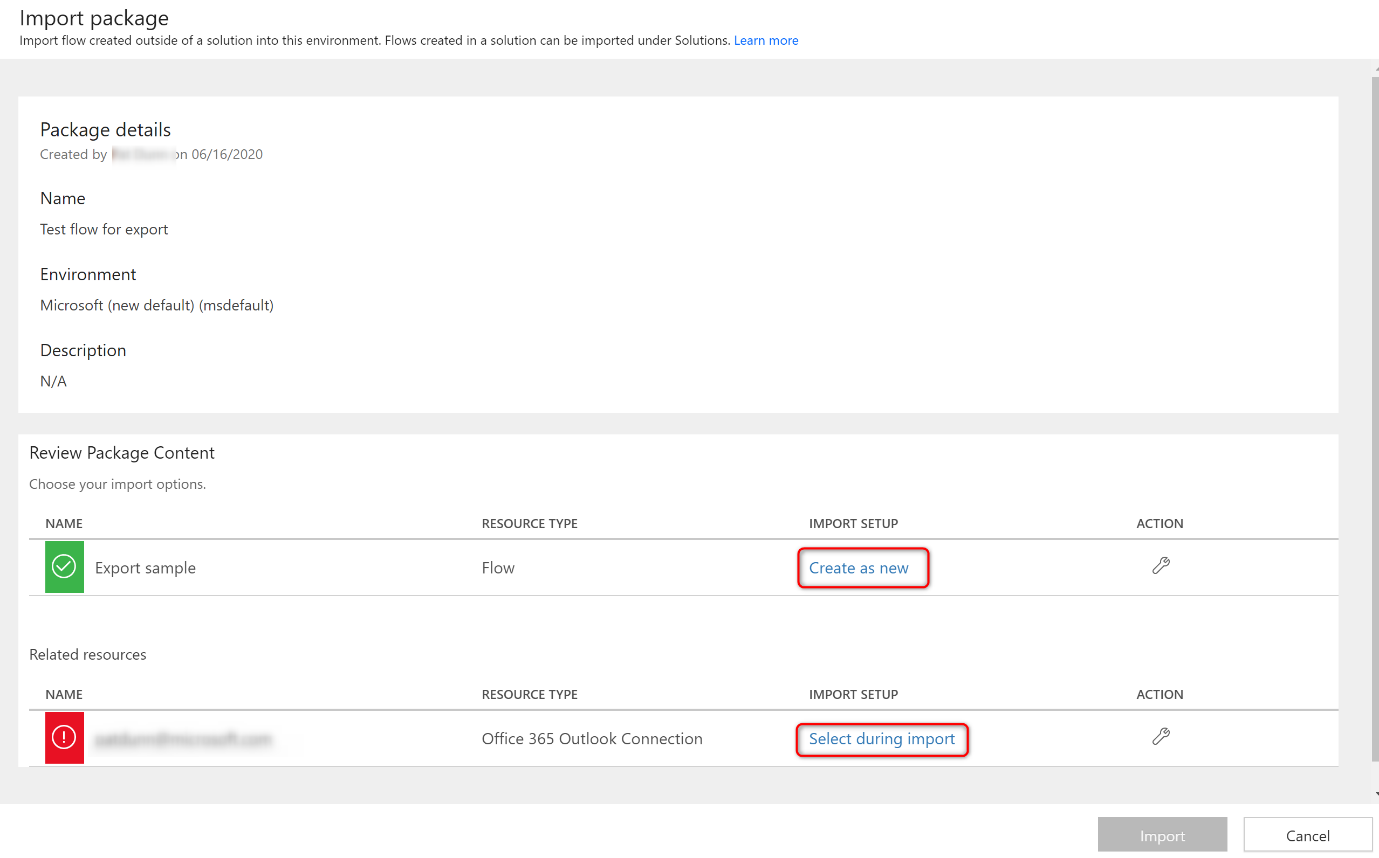
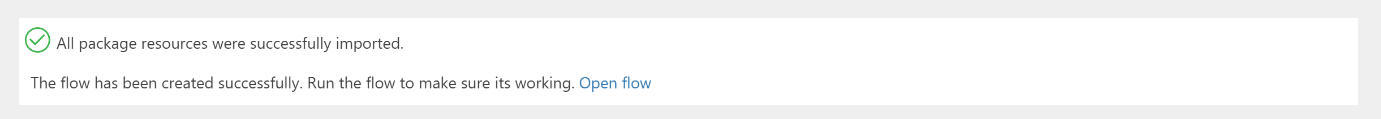
1. On th​e Export Package screen complete the form as follows



**Name -**The name of the export package. Note this won’t be the name of the flow, since the existing name will be used, but just used for the name of the file that will be downloaded.  
**Flow Import Setup** - If the flow will be new in the target environment, then change ‘Update’ to ‘Create as new’  
**Connector Import setup** - Each connector will also be listed, but you won’t be able to change this setting

1. ​​​Click the Export button and a zip file will be downloaded to the Downloads folder of your computer. The file name will be the name you provided above, with the date and UTC time appended  
   
2. Now pick the target environment from the environment dropdown
3. Press the Import button on the top nav. **​Note: If you do not see the Import button, make sure you are at https://flow.microsoft.com not at powerapps.com.**



1. On the Import Package screen, press the Upload button to locate your file from your downloads folder and press OK  
   
2. Now the Import package screen will contain the details of the package. Any red icons need to be fixed before the Import button is available  
     
   **Flow IMPORT SETUP** – Optionally you can click on Create as new to change the name of the flow  
   **Connection IMPORT SEUP** – Click on the Select during import link for each connection to choose an existing connection in this environment or create a new one. Note that you will only be able to select your own connections. If a flow requires other connections, like a service account, you will need to edit the flow later with that account.
3. Press the Import button and your flow will be saved.  
   
4. Click the Open flow link to go to the details page of that flow. You may now edit and share it with others​

​​

# Getting Hel​p

* Have a question about the Power Platform in the Contoso tenant? Please contact **The CONTOSO Power Platform Governance Team**
* Check out the **WW Power Platform Community**! Power Peeps gather here to connect and ask questions. Join to get in on the conversation.
* Want to get better at building Power Apps? Check out the [**Power Apps Learning Path on Microsoft Learn**](https://docs.microsoft.com/en-us/learn/browse/?products=power-platform)
* Is your app going out to a broader audience at Microsoft? Learn how to build enterprise canvas apps with our [**Coding Standards Guide**](https://aka.ms/powerappscanvasguidelines) and [**Accessibility Guide**](https://aka.ms/powerappsaccessibilityguidelines)
* Ask a question on the **Power Apps Yammer forum**. Novices, professionals, and people from the product group come together to discuss all things Power Apps here.
* Need a change to the available connectors in an environment, or do you need an external domain allow-listed? Please contact **Power Automate and Power Apps DLP** at https://<url>