Microsoft

# WorkshopPLUS
# Power Platform for Administrators

Power Platform Policies

# Conditions and terms of use

© Microsoft Corporation. All rights reserved.

You may use these training materials solely for your personal internal reference and non-commercial purposes.  You may not distribute, transmit, resell or otherwise make these training materials available to any other person or party without express permission from Microsoft Corporation.  URL's or other internet website references in the training materials may change without notice.  Unless otherwise noted, any companies, organizations, domain names, e-mail addresses, people, places and events depicted in the training materials are for illustration only and are fictitious. No real association is intended or inferred. THESE TRAINING MATERIALS ARE PROVIDED "AS IS"; MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED IN THESE TRAINING MATERIALS

# Objectives

After completing this Learning, you will be able to:

1

**Understand….**

- ✓ What Power Platform Data Loss Prevention Policies are
- ✓ Who can Create and managed DLP policies
- ✓ How DLP policies are enforced and visible to users
- ✓ What granular DLP controls are
- ✓ DLP management interfaces

2

**Understand….**

- ✓ What tenant isolation policy is
- ✓ Different configuration scenarios for tenant isolation

3

**Understand….**

- ✓ What Customer lockbox is
- ✓ Workflow of customer lockbox once it is configured

4

**Understand….**

- ✓ What Enterprise policies are

5

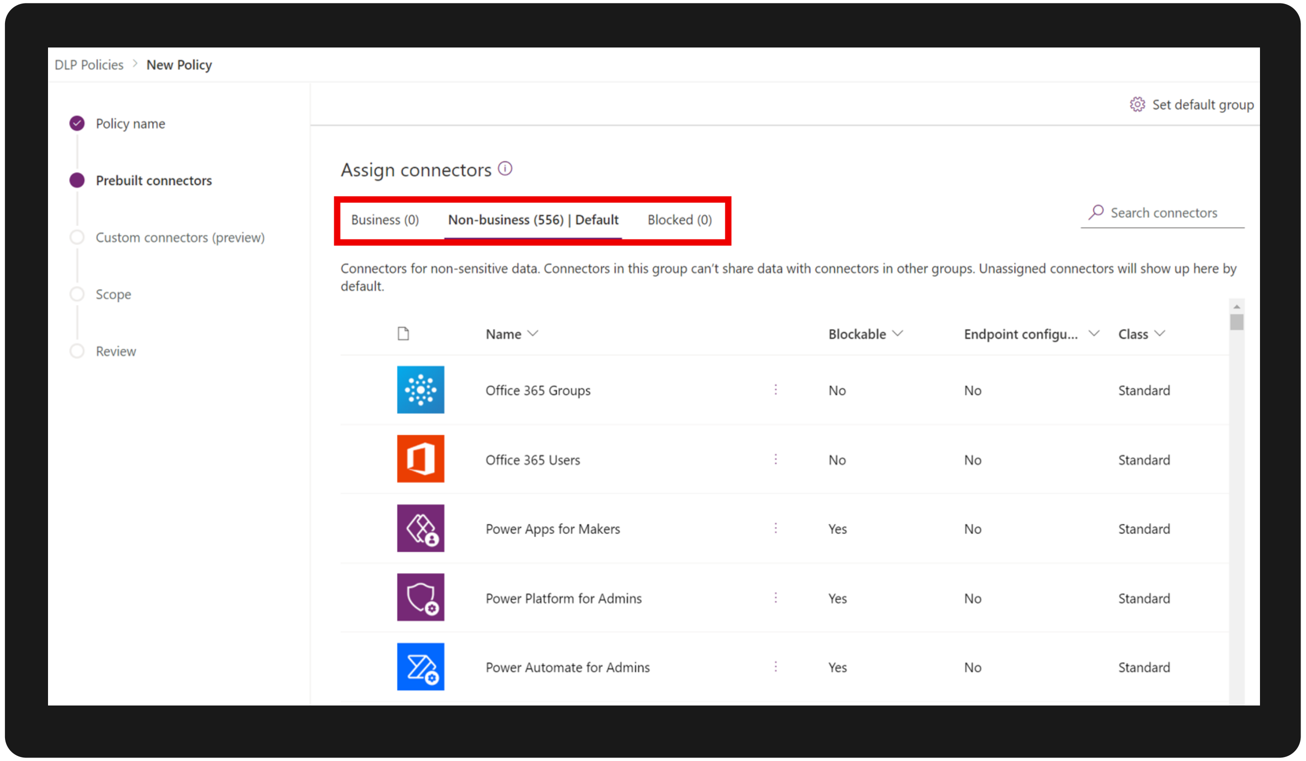
**Understand….**

- ✓ What Billing policies are
- ✓ How Billing policies are configured

# Understand Data Loss Prevention Policies

# What are Data Loss Prevention (DLP) policies?

- Power Platform DLP policies allow you to control data flows across data connectors when used within Power Apps and Power Automate.
- Simply put, DLP enables admins to isolate business data from personal use data within Power Platform.



Connectors for non-sensitive data. Connectors in this group can't share data with connectors in other groups. Unassigned connectors will show up here by default.

| | Name | Blockable | Endpoint configu... | Class |
|---|---|---|---|---|
| | Office 365 Groups | No | No | Standard |
| | Office 365 Users | No | No | Standard |
| | Power Apps for Makers | Yes | No | Standard |
| | Power Platform for Admins | Yes | No | Standard |
| | Power Automate for Admins | Yes | No | Standard |

# Connector Classification

Connectors can be classified across the following groups using DLP policies:

## Business

- A given Power App or Power Automate resource can use one or more connectors from **Business** group
- If a Power App or Power Automate resource uses a **Business** connector, it **cannot** use any **Non-business** connector

## Non-business

- A given Power App or Power Automate resource can use one or more connectors from **Non-business** group
- If a Power App or Power Automate resource uses a **Non-business** connector, it **cannot** use any **Business** connector

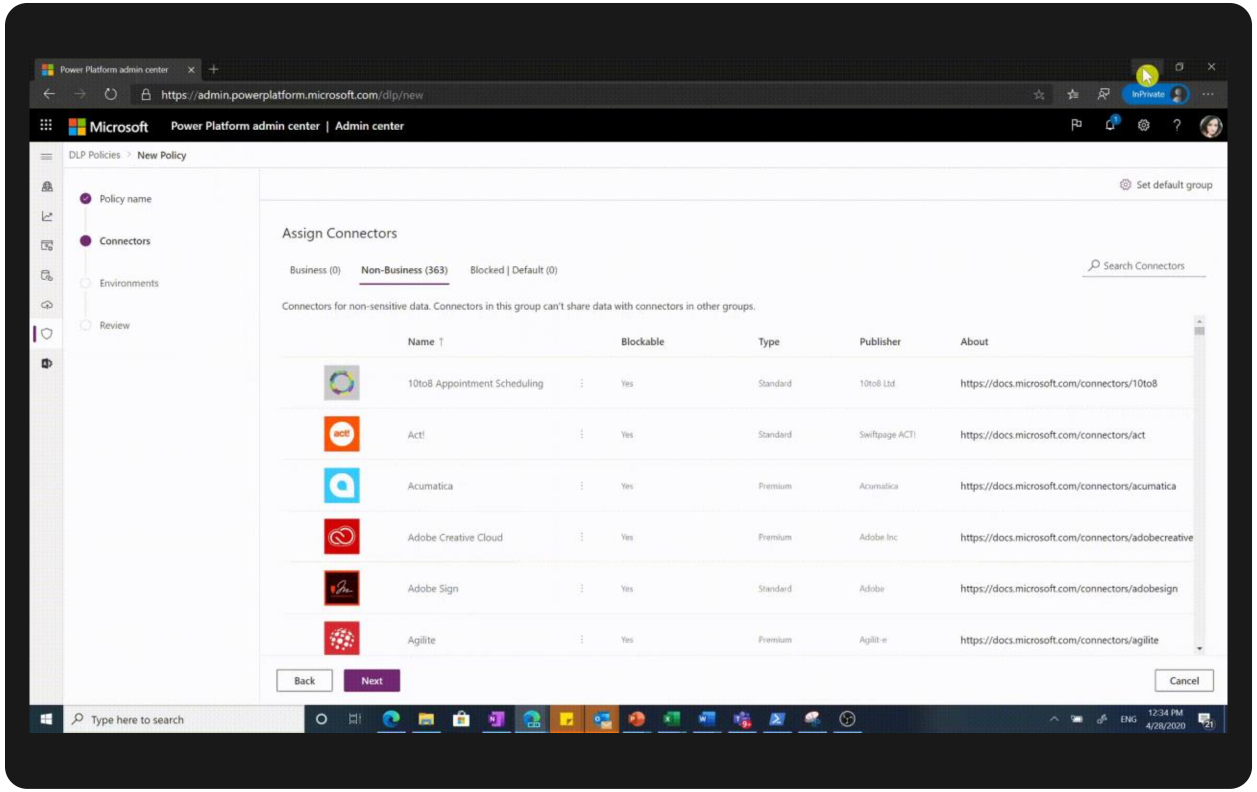
## Blocked

- Any Power App or Power Automate resource cannot use any connector from a **Blocked** group
- All Microsoft owned premium connectors and third-party connectors (standard and premium) can be blocked
- All Microsoft owned standard connectors and Microsoft Dataverse cannot be blocked

# Default Connector Group

**The following grouping logic is applied to new connectors added to Power Platform:**

- Power Platform connector ecosystem keeps evolving and new connectors are added.
- If new connectors are added after DLP policy creation, admins have not had a chance to explicitly categorize them
- These new connectors are automatically added to **Default connector** group identified for them
- Admins can set the **Default connector** group for new connectors in a DLP policy to – Business or Non-business or Blocked
- Admins can review these new connectors retrospectively and classify them explicitly as appropriate
- There are templates in Power Automate for administrators to get alerts when new connectors are added - [Monitor new connectors - Microsoft Power Platform - Power Platform | Microsoft Learn]()



Assign Connectors

Business (0) | Non-Business (363) | Blocked | Default (0)

Connectors for non-sensitive data. Connectors in this group can't share data with connectors in other groups.

| Name ↑ | Blockable | Type | Publisher | About |
|---|---|---|---|---|
| 10to8 Appointment Scheduling | Yes | Standard | 10to8 Ltd | https://docs.microsoft.com/connectors/10to8 |
| Act! | Yes | Standard | Swiftpage ACT! | https://docs.microsoft.com/connectors/act |
| Acumatica | Yes | Premium | Acumatica | https://docs.microsoft.com/connectors/acumatica |
| Adobe Creative Cloud | Yes | Premium | Adobe Inc | https://docs.microsoft.com/connectors/adobecreative |
| Adobe Sign | Yes | Standard | Adobe | https://docs.microsoft.com/connectors/adobesign |
| Agilite | Yes | Premium | Agilit-e | https://docs.microsoft.com/connectors/agilite |

# Tenant and Environment Policies

Power Platform DLP allows admins to create two types of policies

## Tenant level DLP policies

- Supported only for Power Platform, D365 and Global Administrator roles
- Can be applied to one, more than one or all environments at a time
- Can be created without associating any environment
- Can be edited and viewed by any tenant admin
- Connector settings are visible to all relevant environment admins but are not editable by them
- Cannot be used to manage custom connector policies since they are scoped to a specific environment

## Environment level DLP policies

- Supported for **Environment Admin role** associated with the environment
- Can be applied to **only one environment** at a time
- Specifying the environment is mandatory to create the policy
- Can be edited and viewed by any environment admin (of the environment) and tenant admins
- Can be used to manage custom connectors for their environment

# DLP Policy Scopes

## Tenant policies have three scope settings

**All environments**

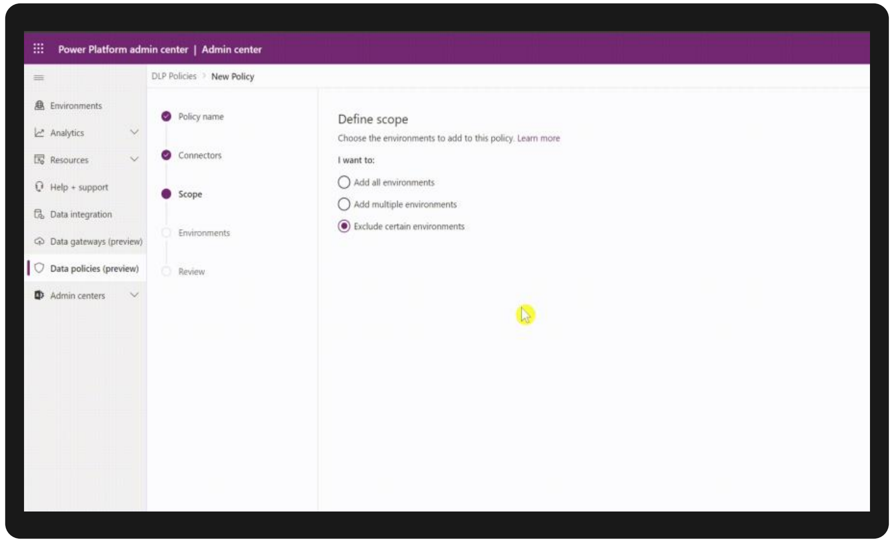
- By default, tenant level policies will be applied to all environments created in the tenant.

**All except selected environments**

- Tenant admins can choose to exclude specific environments to apply the policy.

**Only selected environments**

- Tenant admins can choose to include only specific environments to apply the policy.



Define scope

Choose the environments to add to this policy. Learn more

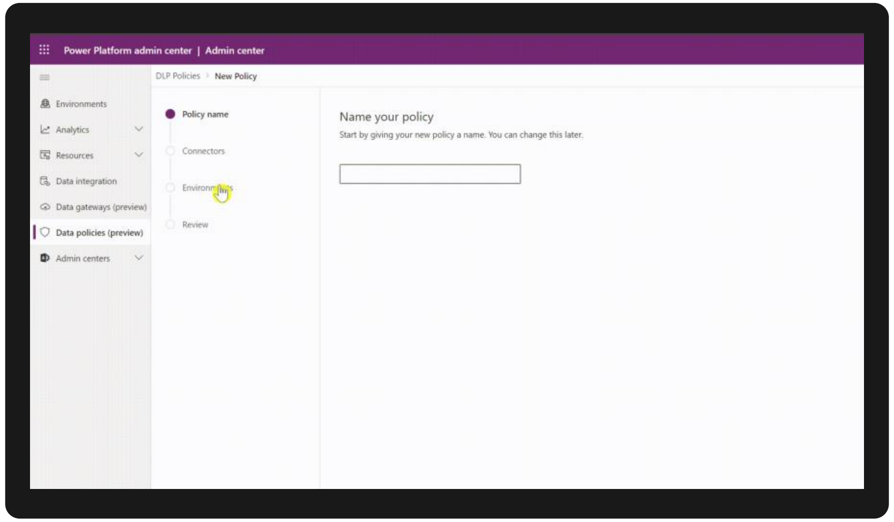
I want to:

○ Add all environments
○ Add multiple environments
● Exclude certain environments

## Environment policies have one scope setting

**One environment only**

Environment admins can choose to apply the policy on one environment at a time.



Name your policy

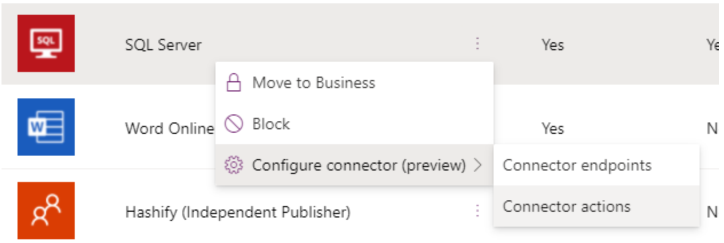
Start by giving your new policy a name. You can change this later.

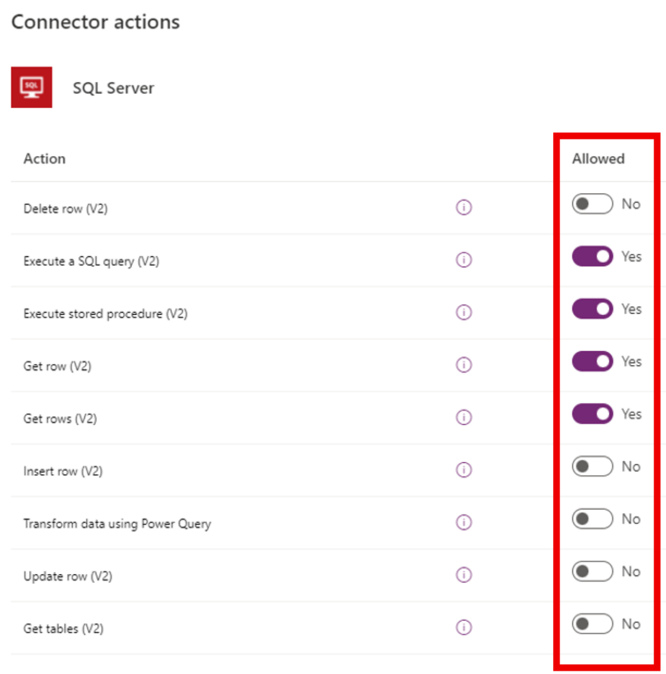
# Connector Action Control

## Granular DLP Controls

- You can use connector action control to allow or block **individual actions** within a given connector.
- On the Connectors page, right-click the connector, and then select Configure connector > Connector actions.
- You can also set the **default value** (Allow or Deny) for any new connector actions that will be added to the connector in the future.

Possible to use PowerShell as well to configure Connector Actions for DLP policies. See more [here]

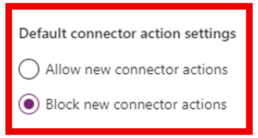




Connector actions

SQL Server

| Action | Allowed |
|---|---|
| Delete row (V2) | No |
| Execute a SQL query (V2) | Yes |
| Execute stored procedure (V2) | Yes |
| Get row (V2) | Yes |
| Get rows (V2) | Yes |
| Insert row (V2) | No |
| Transform data using Power Query | No |
| Update row (V2) | No |
| Get tables (V2) | No |



Default connector action settings

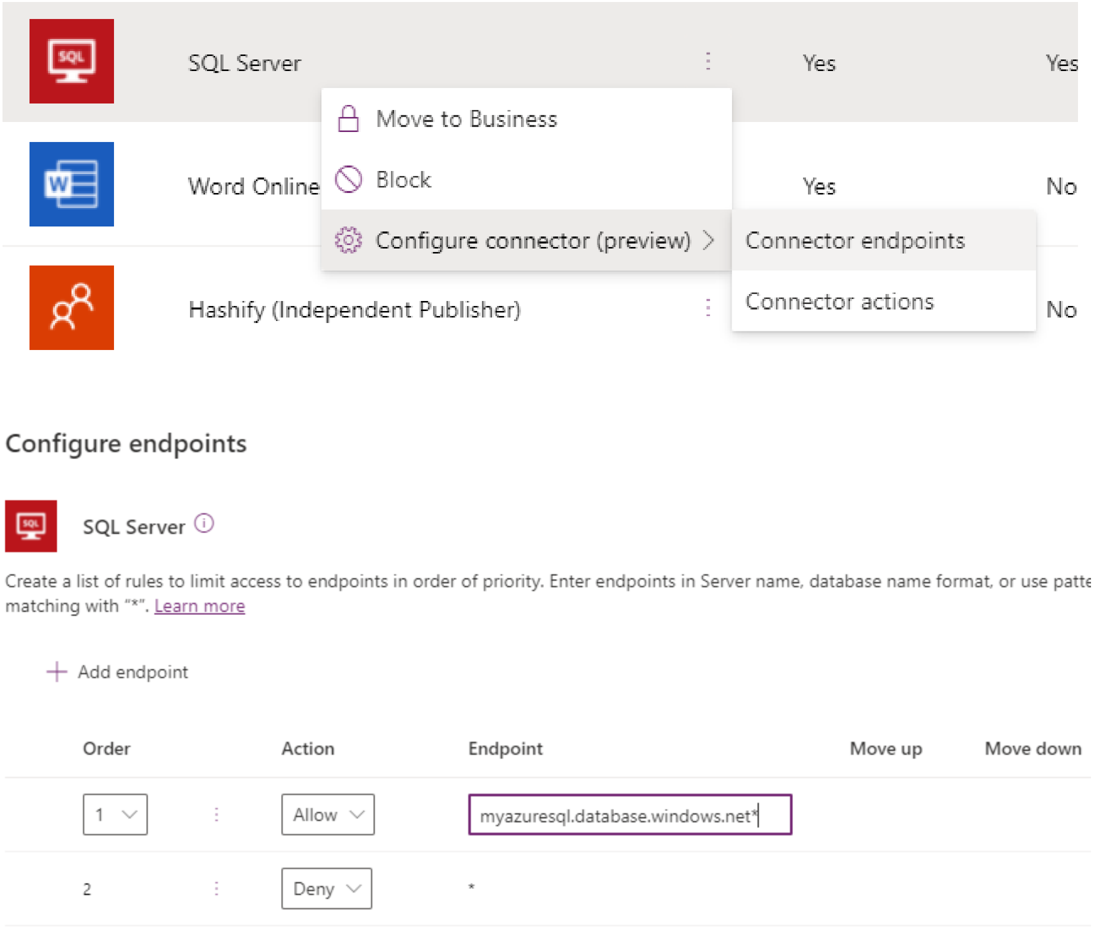
○ Allow new connector actions

● Block new connector actions

# Endpoint Filtering (Preview)

## Granular DLP Controls

- Endpoint filtering allows admins to govern at a fine grain which specific endpoints will be allowed versus blocked at a tenant or environment level.
- This feature is available for HTTP, HTTP with Azure AD, HTTP Webhook, SQL Server, Azure Blob Storage, and SMTP connection endpoints (soon also for Dataverse (legacy)).
- Possible to use PowerShell as well to configure Endpoint Filtering for DLP policies. See more info here



|  |  |  |
|---|---|---|
| SQL Server | Yes | Yes |
| Word Online | Yes | No |
| Hashify (Independent Publisher) |  | No |

Configure endpoints

SQL Server

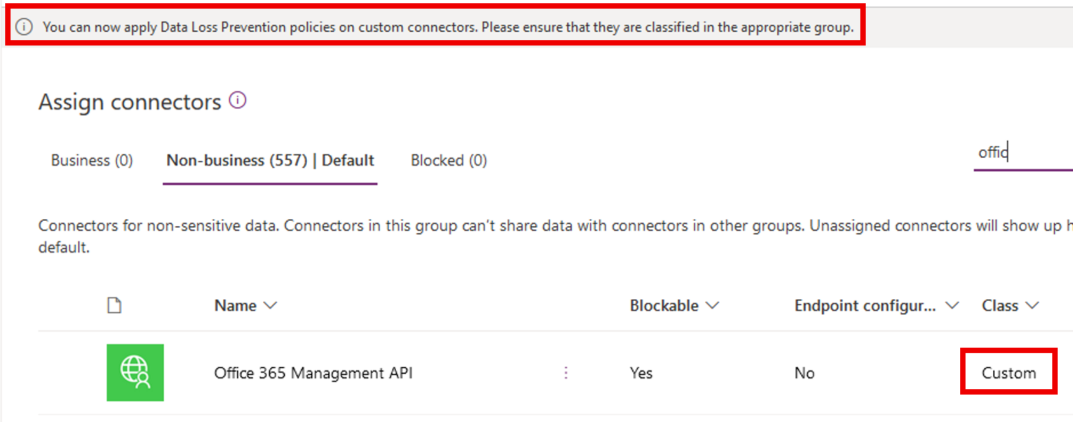
Create a list of rules to limit access to endpoints in order of priority. Enter endpoints in Server name, database name format, or use patte matching with "*". Learn more

| Order | Action | Endpoint | Move up | Move down |
|---|---|---|---|---|
| 1 | Allow | myazuresql.database.windows.net* |  |  |
| 2 | Deny | * |  |  |

# Custom Connector Parity

Power Platform allows you to create and share custom connectors which can be included in tenant and environment level Data Loss Prevention (DLP) policies.

- Environment admins can now see all custom connectors in their environments in DLP wizard in PPAC and classify individual custom connectors by name for environment-level DLP policies.
- Tenant admins see a new tab called **Custom connectors** in DLP wizard in PPAC which allows them to specify an ordered list of Allow and Deny URL patterns for custom connectors.
- The rule for * will always be the last entry in the list which applies to all custom connectors not matched by any previous rule.
- Admins can tag the * pattern to Blocked/Business/Non-business/Ignore. By default, the pattern is set up as Ignore for new DLP policies.

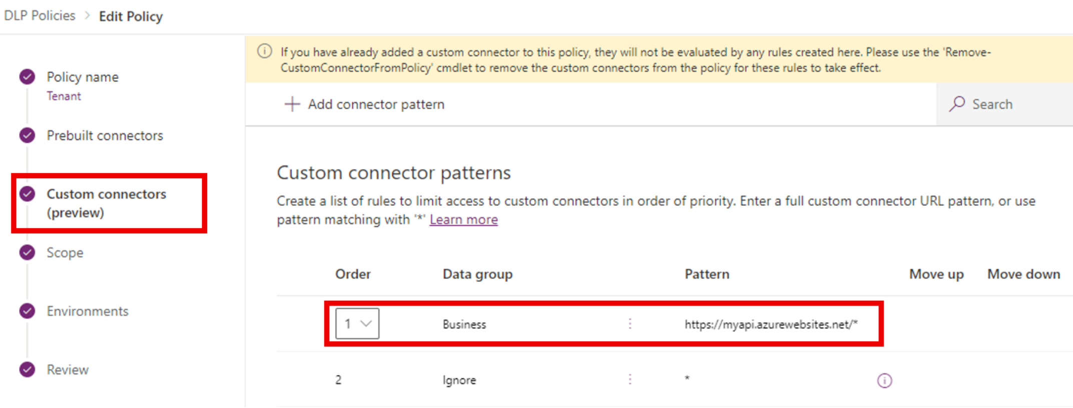


You can now apply Data Loss Prevention policies on custom connectors. Please ensure that they are classified in the appropriate group.

Assign connectors

Connectors for non-sensitive data. Connectors in this group can't share data with connectors in other groups. Unassigned connectors will show up h default.

| | Name | Blockable | Endpoint configur... | Class |
|---|---|---|---|---|
| | Office 365 Management API | Yes | No | Custom |



If you have already added a custom connector to this policy, they will not be evaluated by any rules created here. Please use the 'Remove-CustomConnectorFromPolicy' cmdlet to remove the custom connectors from the policy for these rules to take effect.

Custom connector patterns

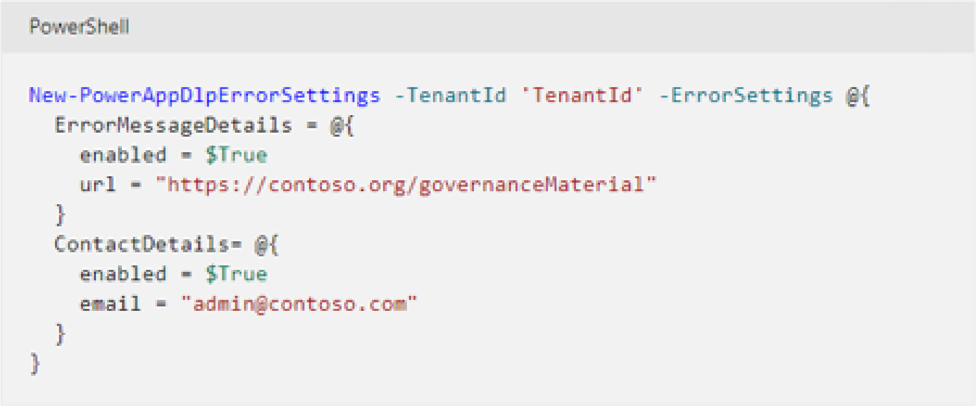
Create a list of rules to limit access to custom connectors in order of priority. Enter a full custom connector URL pattern, or use pattern matching with '*' Learn more

| Order | Data group | Pattern | Move up | Move down |
|---|---|---|---|---|
| 1 | Business | https://myapi.azurewebsites.net/* | | |
| 2 | Ignore | * | | |

DLP for custom connectors

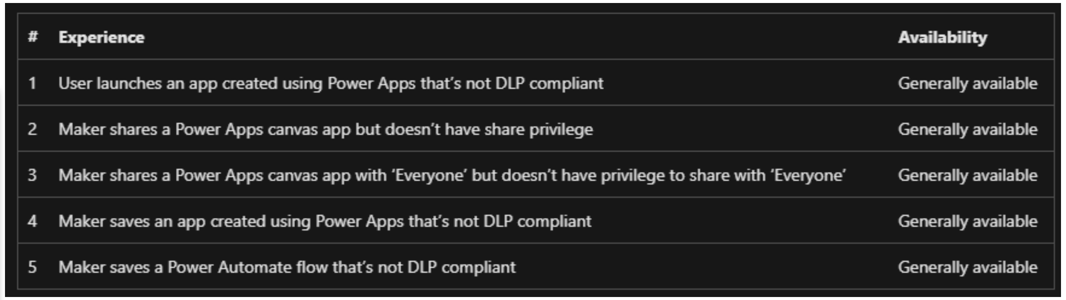
# Custom DLP Governance Error Message

- You can use Power Platform DLP PowerShell commands to set a custom link to lead end users to your organization’s governance documentation and include a governance contact, when they are prompted by governance controls.
- For instance, when the governance error message content is set, it will appear in Power Apps Data Loss Prevention policy runtime enforcement messages.

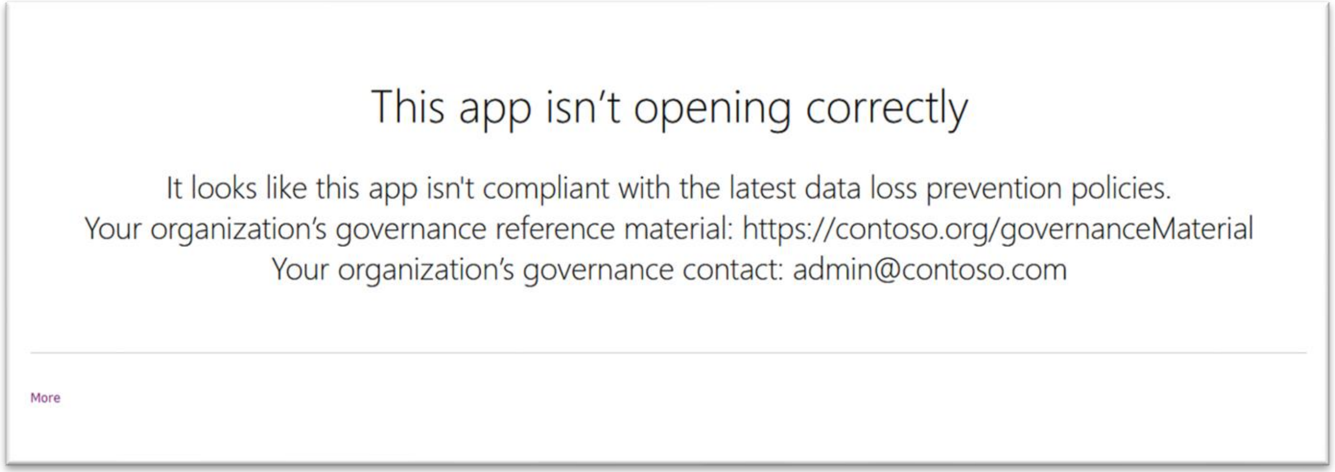


PowerShell

```
New-PowerAppDlpErrorSettings -TenantId 'TenantId' -ErrorSettings @{
  ErrorMessageDetails = @{
    enabled = $True
    url = "https://contoso.org/governanceMaterial"
  }
  ContactDetails= @{
    enabled = $True
    email = "admin@contoso.com"
  }
}
```



| # | Experience | Availability |
|---|---|---|
| 1 | User launches an app created using Power Apps that’s not DLP compliant | Generally available |
| 2 | Maker shares a Power Apps canvas app but doesn’t have share privilege | Generally available |
| 3 | Maker shares a Power Apps canvas app with ‘Everyone’ but doesn’t have privilege to share with ‘Everyone’ | Generally available |
| 4 | Maker saves an app created using Power Apps that’s not DLP compliant | Generally available |
| 5 | Maker saves a Power Automate flow that’s not DLP compliant | Generally available |



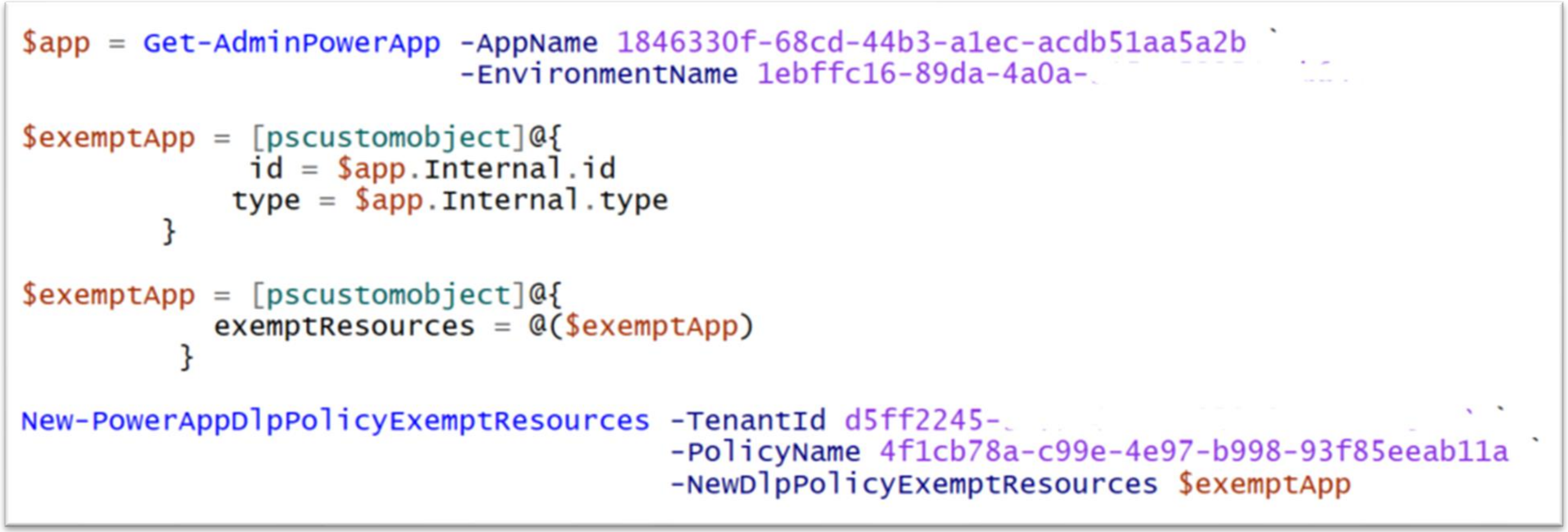
This app isn’t opening correctly

It looks like this app isn't compliant with the latest data loss prevention policies.
Your organization’s governance reference material: https://contoso.org/governanceMaterial
Your organization’s governance contact: admin@contoso.com

Governance error message content commands

# DLP Resource Exemption

- You can use Power Platform DLP PowerShell commands to exempt or unexempt Apps and Flows from DLP policies.
- For example, by using following commands you can exempt App from specified DLP policy.
- **NOTE:** Currently, there is no UI to be able to see all Apps and Flows excluded from the policies, so admins would need to track and monitor excluded resources – you can retrieve list of exempt resources via PowerShell.



```
$app = Get-AdminPowerApp -AppName 1846330f-68cd-44b3-a1ec-acdb51aa5a2b `
                         -EnvironmentName 1ebffc16-89da-4a0a-[redacted]

$exemptApp = [pscustomobject]@{
               id = $app.Internal.id
              type = $app.Internal.type
         }

$exemptApp = [pscustomobject]@{
              exemptResources = @($exemptApp)
          }

New-PowerAppDlpPolicyExemptResources -TenantId d5ff2245-[redacted] `
                                     -PolicyName 4f1cb78a-c99e-4e97-b998-93f85eeab11a `
                                     -NewDlpPolicyExemptResources $exemptApp
```

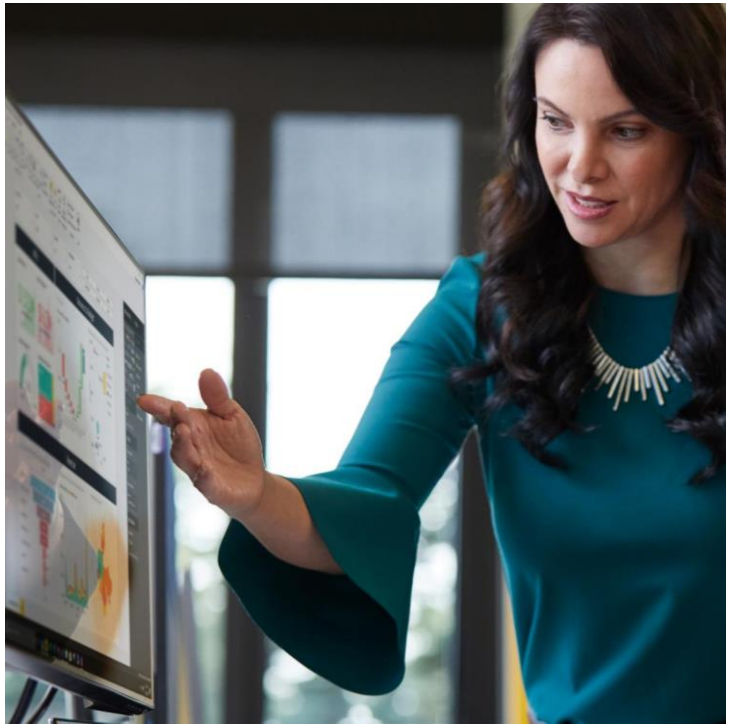
DLP resource exemption cmdlets

# Demonstration

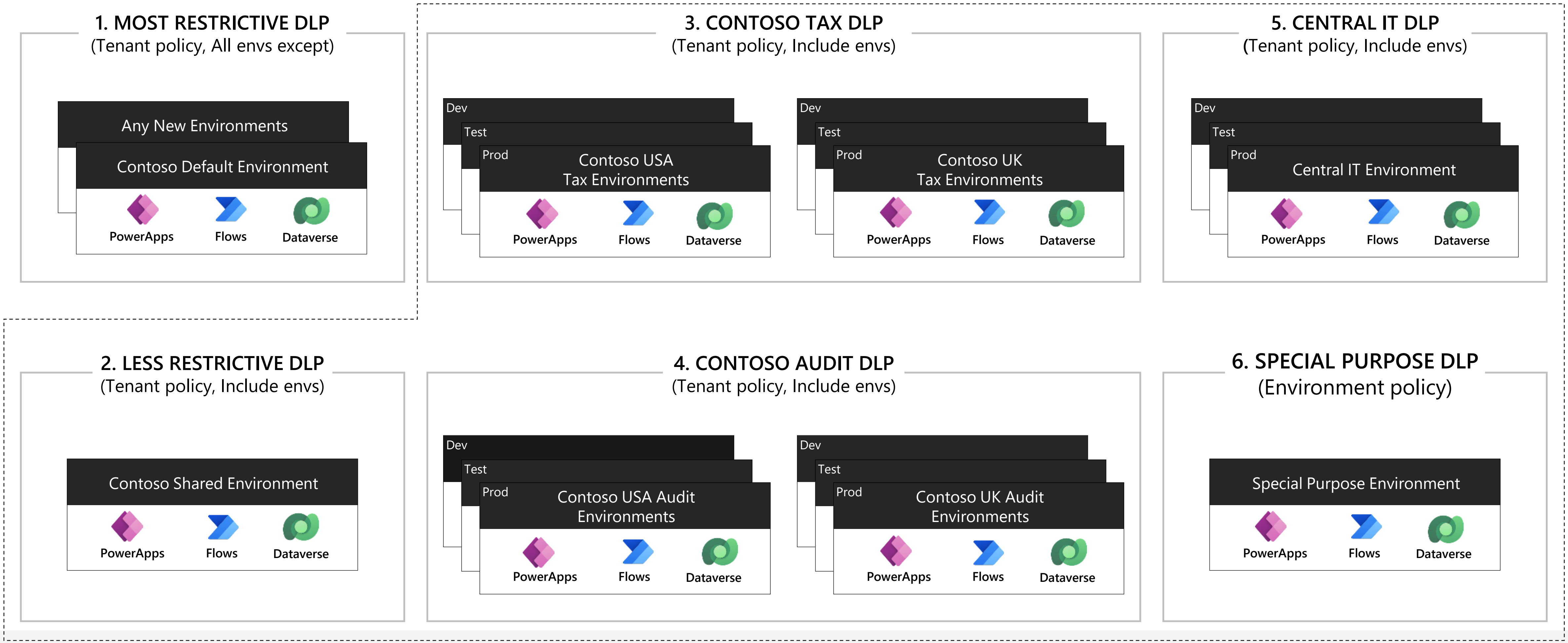
Create tenant level Data Loss Prevention policy

Consider demoing the following:

1. Open PPAC
2. Click **Data Policies** from the left menu
3. Click New Policy
4. Set policy name as "**Tenant Policy**"
5. In the connectors list (Non-Business) filter all non-blockable connectors by settings filter for **Blockable** column with value **No**
6. Select all connectector (about 24) and move them to **Business** group and click **Next**
7. Do not change anything in Custom Connectors page just click **Next**
8. On the Scope page select "**Add all environments**" and click **Next**
9. In the last page click "**Create policy**"



# Example - Contoso Corp DLP policies



**1. MOST RESTRICTIVE DLP**
(Tenant policy, All envs except)

Any New Environments
Contoso Default Environment
PowerApps Flows Dataverse

**3. CONTOSO TAX DLP**
(Tenant policy, Include envs)

Dev
Test
Prod
Contoso USA Tax Environments
PowerApps Flows Dataverse

Dev
Test
Prod
Contoso UK Tax Environments
PowerApps Flows Dataverse

**5. CENTRAL IT DLP**
(Tenant policy, Include envs)

Dev
Test
Prod
Central IT Environment
PowerApps Flows Dataverse

**2. LESS RESTRICTIVE DLP**
(Tenant policy, Include envs)

Contoso Shared Environment
PowerApps Flows Dataverse

**4. CONTOSO AUDIT DLP**
(Tenant policy, Include envs)

Dev
Test
Prod
Contoso USA Audit Environments
PowerApps Flows Dataverse

Dev
Test
Prod
Contoso UK Audit Environments
PowerApps Flows Dataverse

**6. SPECIAL PURPOSE DLP**
(Environment policy)

Special Purpose Environment
PowerApps Flows Dataverse

Centralize DLP Policy management using tenant level policies. Use restrictive policies on shared environments like default environment. Create minimal number of policies per environment. There is no strict hierarchy between tenant and environment policies.

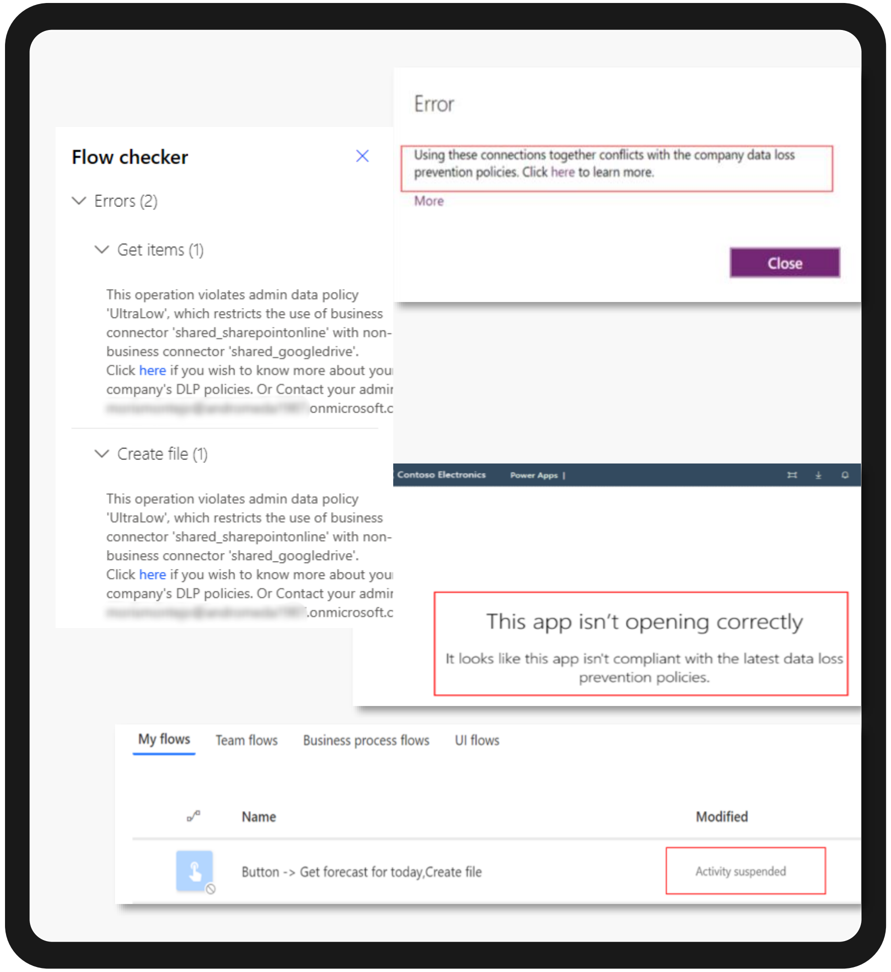
# DLP Policy Enforcement

## Design-time

- Power Apps makers see an error upon using connectors that don't belong together or are blocked using DLP policies. Apps violating DLP policies cannot be saved at design time unless DLP violation is resolved.
- Power Automate makers see a warning while saving a flow using connectors that don't belong together or are blocked using DLP policies. You can save the flow but **not able to run**

## Run-time

- If DLP policy changes impact an existing Power App negatively and it becomes non-compliant, then users are no longer able to launch it and get an error.
- If DLP policy changes impact an existing Power Automate negatively and it becomes non-compliant, then it is automatically marked as suspended users are no longer able to execute it. Power Automate suspension may take ~5 mins to come into effect after policy changes.



This operation violates admin data policy 'UltraLow', which restricts the use of business connector 'shared_sharepointonline' with non-business connector 'shared_googledrive'. Click here if you wish to know more about you company's DLP policies. Or Contact your admi [redacted] onmicrosoft.c

This operation violates admin data policy 'UltraLow', which restricts the use of business connector 'shared_sharepointonline' with non-business connector 'shared_googledrive'. Click here if you wish to know more about you company's DLP policies. Or Contact your admi [redacted].onmicrosoft.c

Using these connections together conflicts with the company data loss prevention policies. Click here to learn more.

This app isn't opening correctly

It looks like this app isn't compliant with the latest data loss prevention policies.

| Name | Modified |
|---|---|
| Button -> Get forecast for today,Create file | Activity suspended |

# Multiple Policy Impact on Environments

If multiple tenant or environment level policies are applied simultaneously on an environment, then the **most restrictive rules accrue.**

## Blocked connectors

- If a connector is marked as ‘blocked’ in **any** one DLP policy applied to the environment, then the net outcome is that this connector is blocked from usage within the environment.
- It doesn’t matter if other DLP policies applied to the environment mark it as business or non-business.

## Business/Non-Business connectors

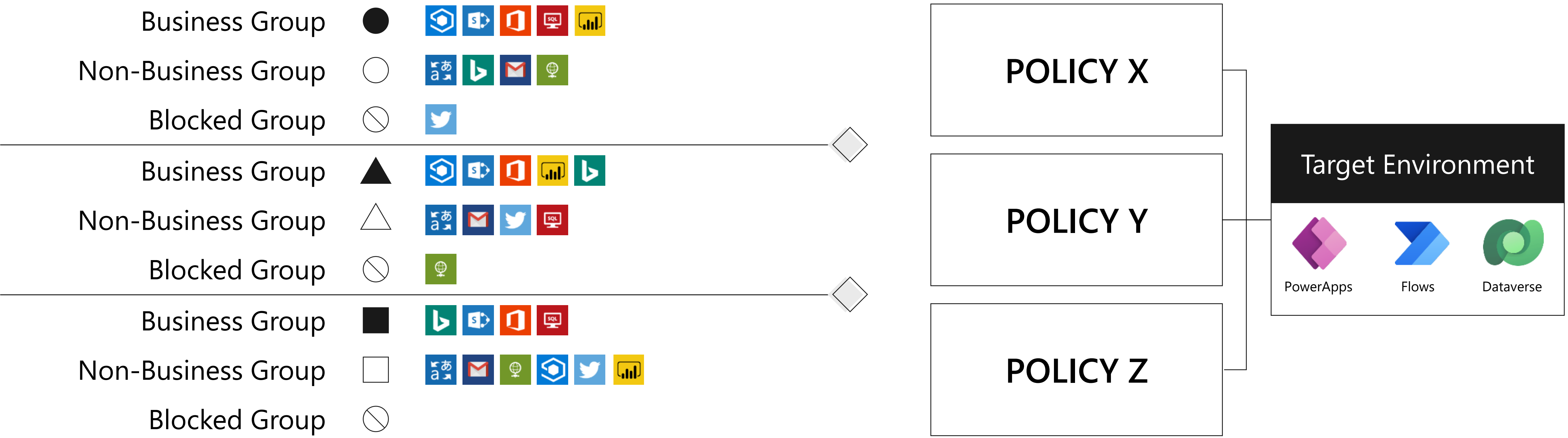
If all DLP policies applied to the environment mark a certain set of connectors as business or non-business, then the most restrictive groupings define what connectors can be used together vs. Not.

For example

Policy X = B {1,2,3} NB {4,5} ; Policy Y = B {3,4,5} NB {1,2}

Then – Net outcome : {1,2} {3} {4,5}

# Multiple DLP Policies – Example Scenario



Business Group ●

Non-Business Group ○

Blocked Group ⊘

Business Group ▲

Non-Business Group △

Blocked Group ⊘

Business Group ■

Non-Business Group □

Blocked Group ⊘

POLICY X

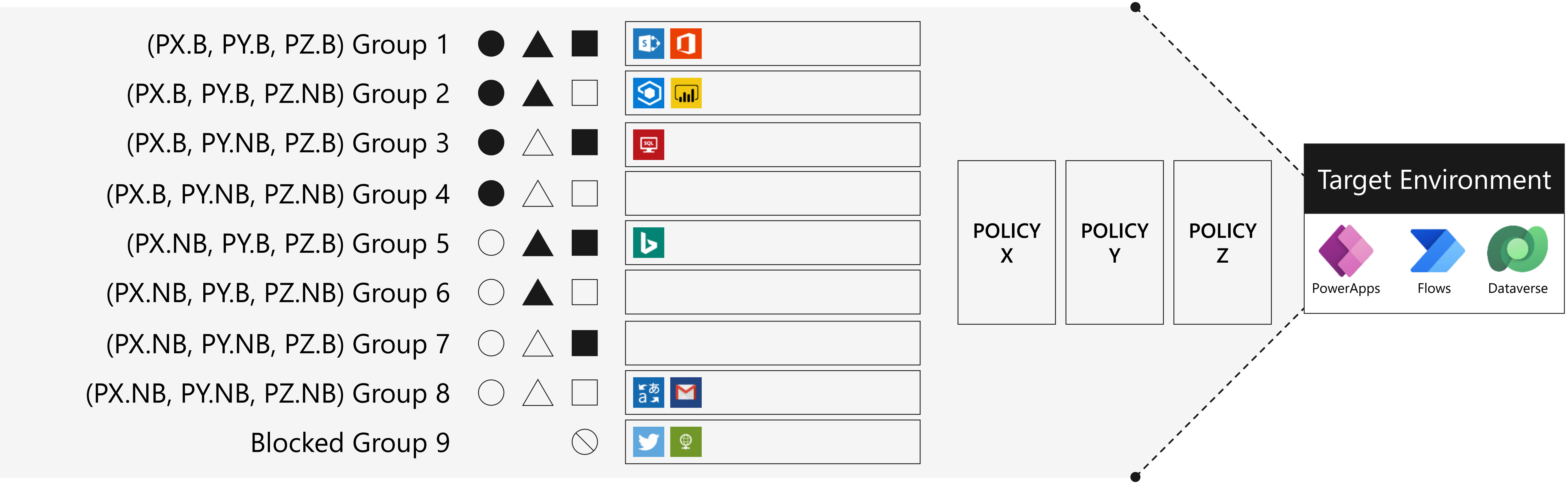
POLICY Y

POLICY Z

Target Environment

**Multiple DLP policies applied to the same environment grouping connectors across Business/Non-business/Blocked. This set up makes the outcome of what connectors can be used together – Fragmented and hard to predict**

# Multiple DLP Policies – Net Outcome



| | | | |
|---|---|---|---|
| (PX.B, PY.B, PZ.B) Group 1 | ● | ▲ | ■ |
| (PX.B, PY.B, PZ.NB) Group 2 | ● | ▲ | □ |
| (PX.B, PY.NB, PZ.B) Group 3 | ● | △ | ■ |
| (PX.B, PY.NB, PZ.NB) Group 4 | ● | △ | □ |
| (PX.NB, PY.B, PZ.B) Group 5 | ○ | ▲ | ■ |
| (PX.NB, PY.B, PZ.NB) Group 6 | ○ | ▲ | □ |
| (PX.NB, PY.NB, PZ.B) Group 7 | ○ | △ | ■ |
| (PX.NB, PY.NB, PZ.NB) Group 8 | ○ | △ | □ |
| Blocked Group 9 | | | ⊘ |

POLICY X

POLICY Y

POLICY Z

Target Environment

PowerApps

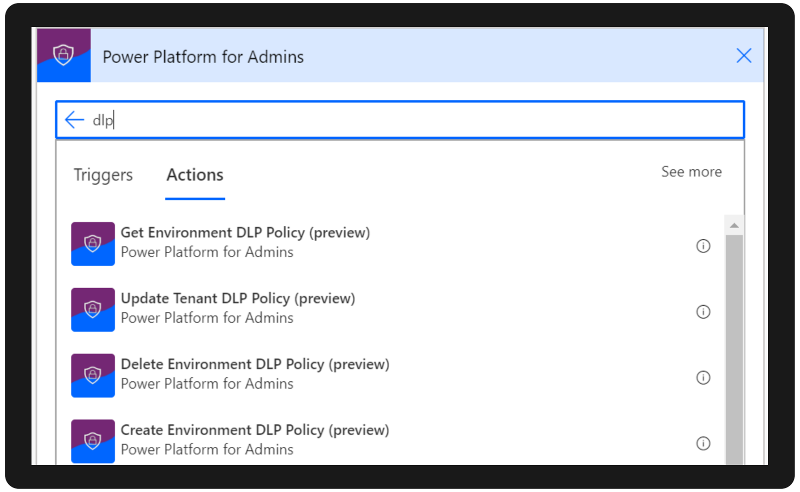
Flows

Dataverse

All blocked connectors map to blocked. For business/non-business - 3 policies will fragment connector grouping outcome into as many as 3^2 = 8 different sets

For predictable outcomes use minimal number of DLP policies per environment

# DLP Management Interfaces



Power Platform for Admins

← dlp

Triggers | Actions | See more

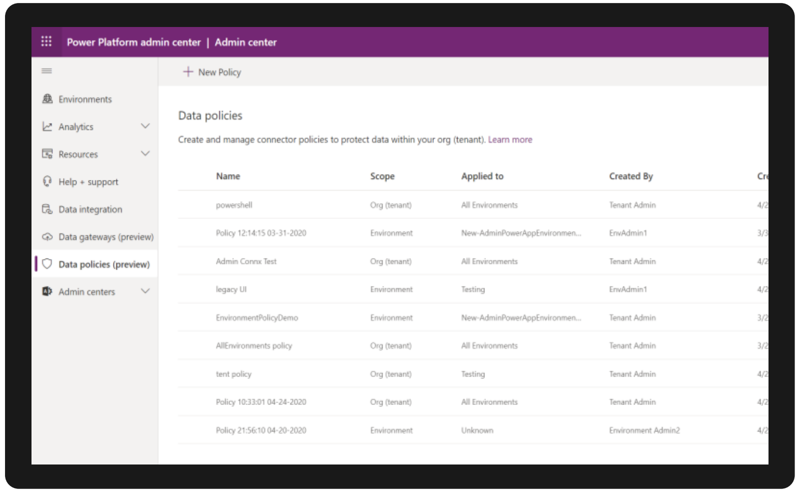
Get Environment DLP Policy (preview)
Power Platform for Admins

Update Tenant DLP Policy (preview)
Power Platform for Admins

Delete Environment DLP Policy (preview)
Power Platform for Admins

Create Environment DLP Policy (preview)
Power Platform for Admins

Power Platform for Admins Connector

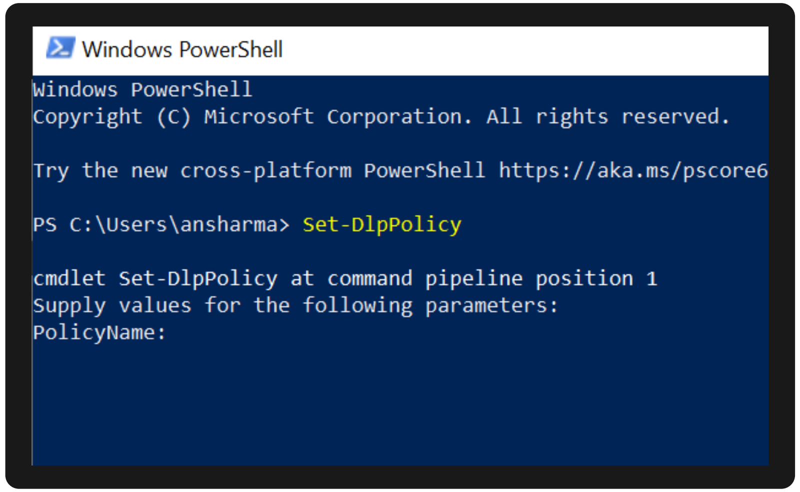


Data policies

Create and manage connector policies to protect data within your org (tenant). Learn more

| Name | Scope | Applied to | Created By | Cr |
|---|---|---|---|---|
| powershell | Org (tenant) | All Environments | Tenant Admin | 4/2 |
| Policy 12:14:15 03-31-2020 | Environment | New-AdminPowerAppEnvironmen... | EnvAdmin1 | 3/3 |
| Admin Connx Test | Org (tenant) | All Environments | Tenant Admin | 4/2 |
| legacy UI | Environment | Testing | EnvAdmin1 | 4/2 |
| EnvironmentPolicyDemo | Environment | New-AdminPowerAppEnvironmen... | Tenant Admin | 3/2 |
| AllEnvironments policy | Org (tenant) | All Environments | Tenant Admin | 3/2 |
| tent policy | Org (tenant) | Testing | Tenant Admin | 4/2 |
| Policy 10:33:01 04-24-2020 | Org (tenant) | All Environments | Tenant Admin | 4/2 |
| Policy 21:56:10 04-20-2020 | Environment | Unknown | Environment Admin2 | 4/2 |

Power Platform Admin Center



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\ansharma> Set-DlpPolicy

cmdlet Set-DlpPolicy at command pipeline position 1
Supply values for the following parameters:
PolicyName:
```

Power Apps PowerShell

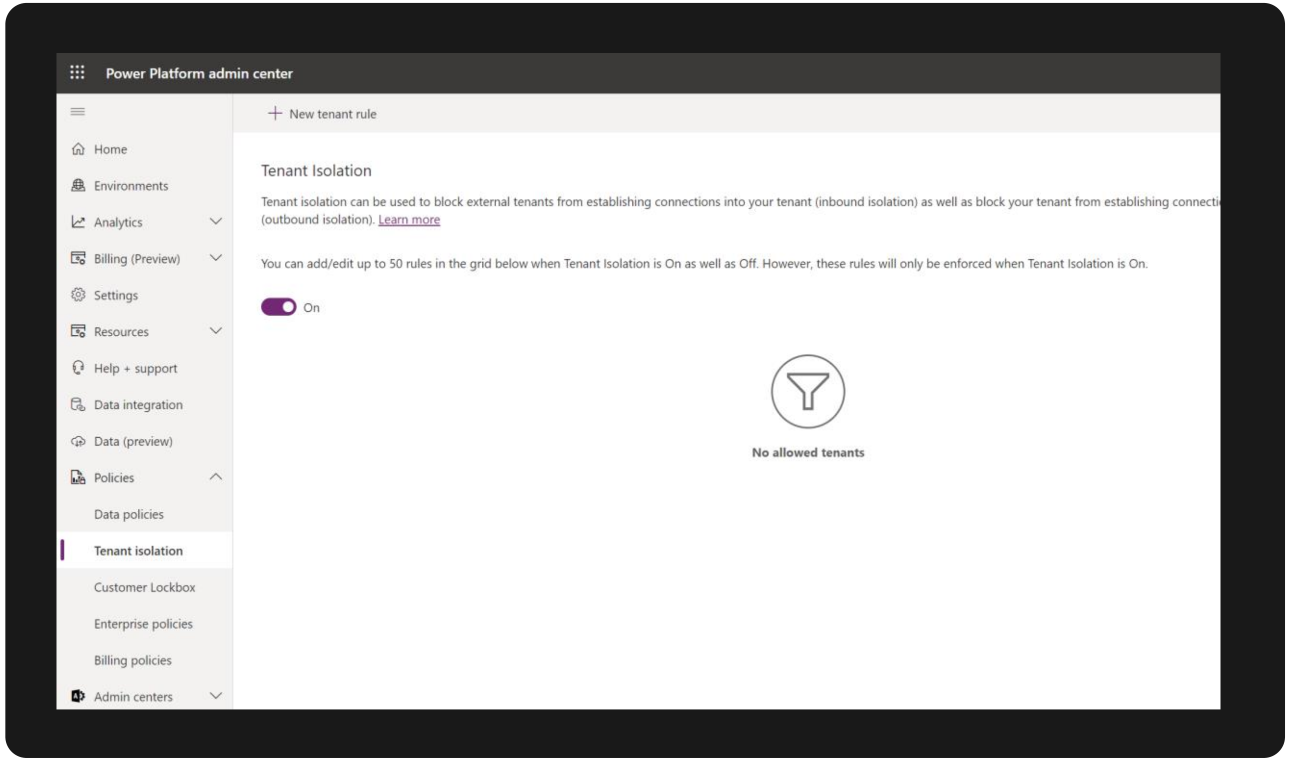
# Tenant Isolation

# Tenant Isolation

*This restriction only applies to PowerApps and Power Automate*

Tenant isolation allows admins to effectively govern the movement of tenant data from Azure AD authorized data sources to and from their tenant.

- Currently in preview and available in Power PPAC > **Policies** > **Tenant isolation**. (Default setting is off).
- New Tenant Rule can be created for Inbound and/or Outbound Restriction once Tenant Isolation is turned on.
- Tenant domain or ID to be added to the Allowed list, you can use * for all tenants.
- Users who create or edit a resource affected by the tenant isolation policy will see a related error message.
- Existing Apps or flows that are in violation of the tenant isolation policy won't run successfully.
- Additional information.



Tenant Isolation

Tenant isolation can be used to block external tenants from establishing connections into your tenant (inbound isolation) as well as block your tenant from establishing connecti (outbound isolation). Learn more

You can add/edit up to 50 rules in the grid below when Tenant Isolation is On as well as Off. However, these rules will only be enforced when Tenant Isolation is On.

● On

No allowed tenants

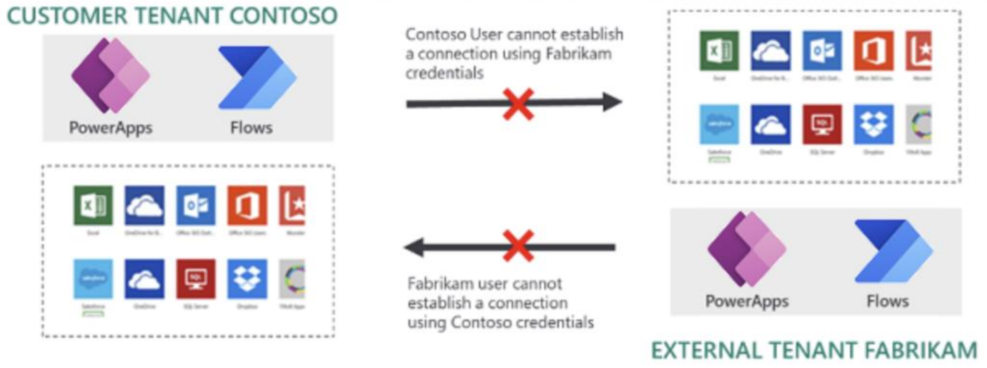
# Configuration scenarios

*This restriction only applies to PowerApps and Power Automate*

- **Two-way tenant isolation (inbound and outbound connection restriction).**
  - Two-way tenant isolation will block connection establishment attempts to your tenant from other tenants. Additionally, two-way tenant isolation will also block connection establishment attempts from your tenant to other tenants.
- **Tenant isolation with allowlists**
  - One-Way tenant isolation or inbound isolation will block connection establishments attempts to your tenant from other tenants.
  - **Scenario: Outbound allowlist** – Fabrikam is added to outbound allowlist of the Contoso tenant.
  - **Scenario: Bidirectional allowlist** – Fabrikam is added to the inbound and outbound allowlists of the Contoso tenant

Note: a connection attempt initiated by a guest user from their host tenant targeting data sources withing the same host tenant is not evaluated by the tenant isolation rules.

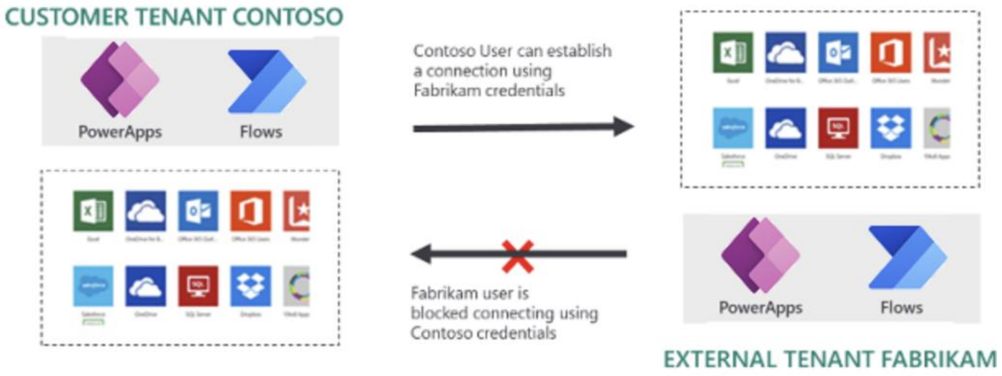
**Two-way tenant isolation (inbound and outbound connection restriction).**



Contoso User cannot establish a connection using Fabrikam credentials

Fabrikam user cannot establish a connection using Contoso credentials

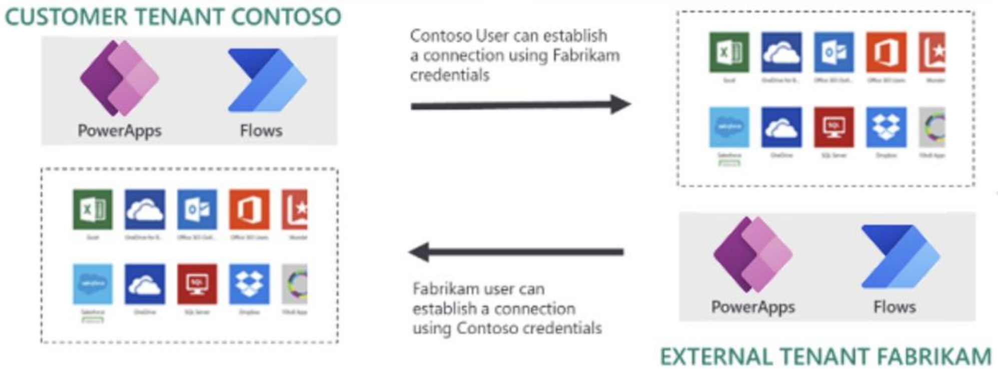
**Scenario: Outbound allowlist**



Contoso User can establish a connection using Fabrikam credentials

Fabrikam user is blocked connecting using Contoso credentials

**Scenario: Bidirectional allowlist**



Contoso User can establish a connection using Fabrikam credentials

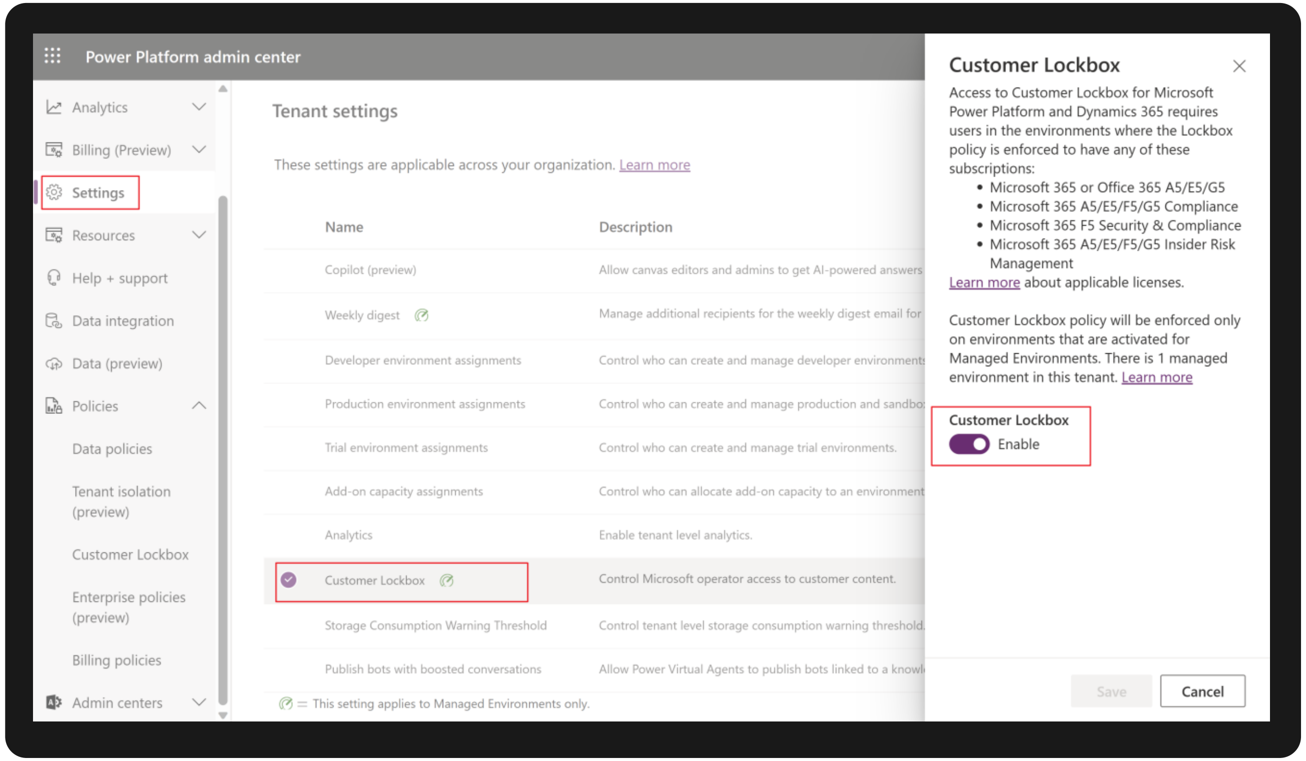
Fabrikam user can establish a connection using Contoso credentials

# Customer Lockbox

# Customer Lockbox

Most operations, support, and troubleshooting performed by Microsoft personnel (including sub-processors) don't require access to customer data. With Power Platform Customer Lockbox, we provide an interface for the customers to review and approve (or reject) data access requests in the **rare** occasion when data access to customer data is needed. It's used in cases where a Microsoft engineer needs to access customer data, whether in response to a customer-initiated support ticket or a problem identified by Microsoft.

- Power Platform applications and services store customer data in several Azure storage technologies. When Customer Lockbox is enabled for an environment, customer data associated with the respective environment is protected by the lockbox policy, irrespective of the storage type.
- To enable, go to **PPAC** > **Settings** > **Customer** Lockbox
- Enabling Customer Lockbox will enforce the policy **only for [Managed Environments].**
- All updates to a lockbox request are recorded and made available via audit logs - [Audit lockbox requests].



Tenant settings

These settings are applicable across your organization. Learn more

| Name | Description |
|---|---|
| Copilot (preview) | Allow canvas editors and admins to get AI-powered answers |
| Weekly digest | Manage additional recipients for the weekly digest email for |
| Developer environment assignments | Control who can create and manage developer environments |
| Production environment assignments | Control who can create and manage production and sandbo |
| Trial environment assignments | Control who can create and manage trial environments. |
| Add-on capacity assignments | Control who can allocate add-on capacity to an environment |
| Analytics | Enable tenant level analytics. |
| Customer Lockbox | Control Microsoft operator access to customer content. |
| Storage Consumption Warning Threshold | Control tenant level storage consumption warning threshold. |
| Publish bots with boosted conversations | Allow Power Virtual Agents to publish bots linked to a knowl |

= This setting applies to Managed Environments only.

Customer Lockbox

Access to Customer Lockbox for Microsoft Power Platform and Dynamics 365 requires users in the environments where the Lockbox policy is enforced to have any of these subscriptions:

- Microsoft 365 or Office 365 A5/E5/G5
- Microsoft 365 A5/E5/F5/G5 Compliance
- Microsoft 365 F5 Security & Compliance
- Microsoft 365 A5/E5/F5/G5 Insider Risk Management

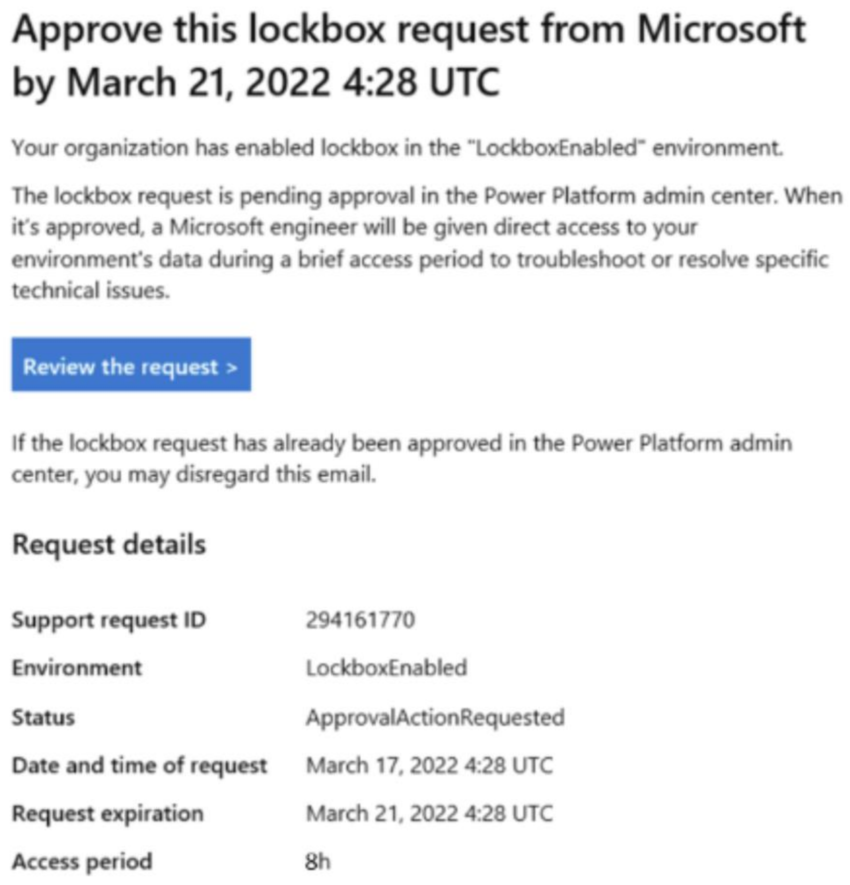
Learn more about applicable licenses.

Customer Lockbox policy will be enforced only on environments that are activated for Managed Environments. There is 1 managed environment in this tenant. Learn more

Customer Lockbox
● Enable

# Customer Lockbox - Workflow

1. Org has an **issue** and **opens case** with **MS Support**.
2. MS reviews/troubleshoots the case and **determines access to customer data is needed** – MS triggers internal process for access to customer data, irrespective of lockbox policy being enabled or not.
3. A **lockbox request is generated** if the respective environment is protected by lockbox policy. **Email is sent** to Global Admin and Power Platform Admin.
4. The approver signs into PPAC and **approves** the request. *The request times out within four days, and no access is granted to MS.*
5. After request is approved, MS obtains **elevated permissions** and fixes the issue. *MS engineers have 8 hours to fix the issue, after which access is revoked.*



## Approve this lockbox request from Microsoft by March 21, 2022 4:28 UTC

Your organization has enabled lockbox in the "LockboxEnabled" environment.

The lockbox request is pending approval in the Power Platform admin center. When it's approved, a Microsoft engineer will be given direct access to your environment's data during a brief access period to troubleshoot or resolve specific technical issues.

If the lockbox request has already been approved in the Power Platform admin center, you may disregard this email.

### Request details

| | |
|---|---|
| Support request ID | 294161770 |
| Environment | LockboxEnabled |
| Status | ApprovalActionRequested |
| Date and time of request | March 17, 2022 4:28 UTC |
| Request expiration | March 21, 2022 4:28 UTC |
| Access period | 8h |

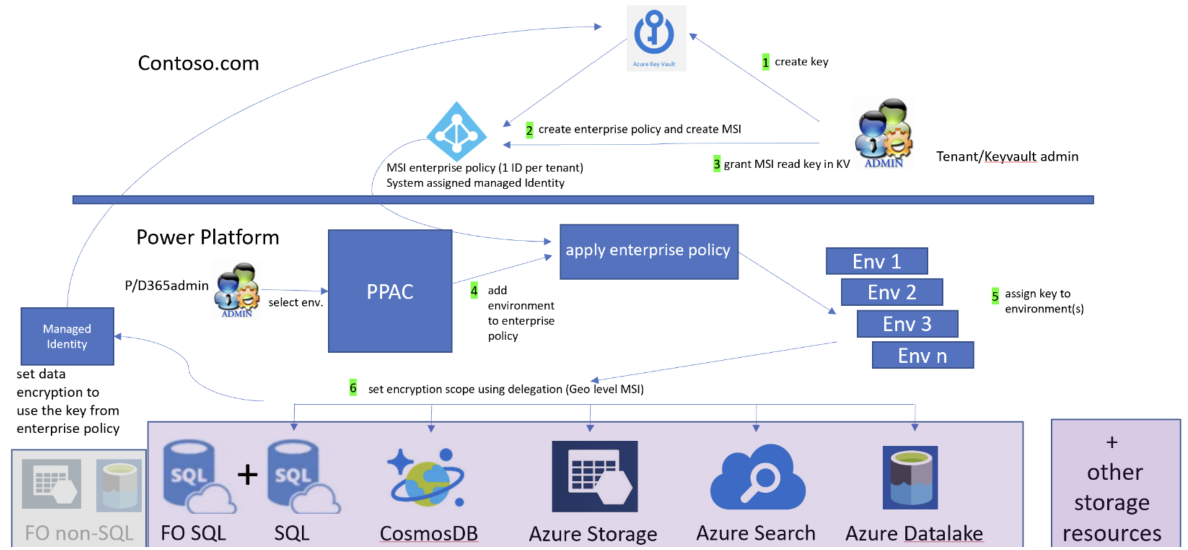
# Enterprise Policies

# Enterprise Policies – CMK – what is it?

CMK = Customer Managed Key

- Customers have **data privacy** and **compliance requirements** to secure their data by **encrypting their data at-rest**.
- Data is secure from exposure in an event where a copy of the database is stolen.
- With **data encryption at-rest**, the stolen database data is protected from being restored to a different server without the **encryption key**.
- All customer data stored in Power Platform is **encrypted at-rest** with strong **Microsoft-managed encryption keys** by **default**.
    - Microsoft stores and manages the database encryption key for all data, so customers don't have to.
- What benefits does a Power Platform customer managed key (CMK) provide?
    - Added data protection control to self-manage the database encryption key associated with Microsoft Dataverse environment(s).
    - Allows you to **rotate** or **swap** the encryption **key on demand.**
    - Allows you to **prevent Microsoft's access** to your customer data when you revoke the key access to our services at any time.

## Customer Managed Key (CMK)



Contoso.com
Azure Key Vault
1 create key
2 create enterprise policy and create MSI
3 grant MSI read key in KV
ADMIN
Tenant/Keyvault admin
MSI enterprise policy (1 ID per tenant)
System assigned managed Identity
Power Platform
P/D365admin
ADMIN
select env.
PPAC
apply enterprise policy
4 add environment to enterprise policy
Env 1
Env 2
Env 3
Env n
5 assign key to environment(s)
Managed Identity
set data encryption to use the key from enterprise policy
6 set encryption scope using delegation (Geo level MSI)
FO non-SQL
SQL
FO SQL
+
SQL
CosmosDB
Azure Storage
Azure Search
Azure Datalake
+ other storage resources

***Currently, all your customer data stored only in the following apps and services can be encrypted with customer-managed key***:

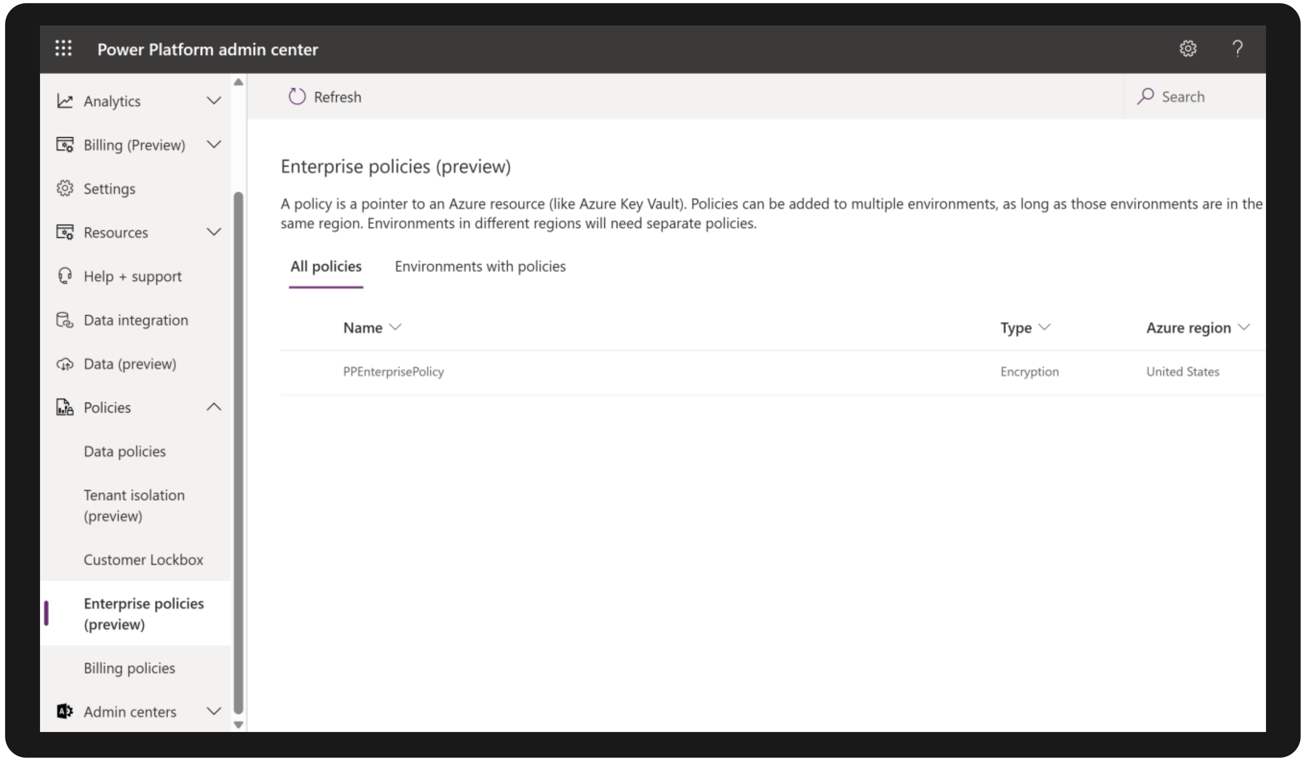
•Dataverse (Custom solutions and Microsoft services)
•Power Automate 1
•Chat for Dynamics 365
•Dynamics 365 Sales
•Dynamics 365 Customer Service
•Dynamics 365 Customer Insights
•Dynamics 365 Omnichannel
•Dynamics 365 Commerce (Finance and operations)
•Dynamics 365 Field Service
•Dynamics 365 Retail
•Dynamics 365 Finance (Finance and operations)
•Dynamics 365 Intelligent Order Management (Finance and operations)
•Dynamics 365 Project Operations (Finance and operations)
•Dynamics 365 Supply Chain Management (Finance and operations)
•Dynamics 365 Fraud Protection (Finance and operations)

# Configuring Enterprise Policies

***Understand the potential risk when you manage your key** - As with any business-critical application, personnel within your organization who have administrative-level access must be trusted. Before you use the key management feature, you should understand the risk when you manage your database encryption keys. It's conceivable that a malicious administrator (a person who is granted or has gained administrator-level access with intent to harm an organization's security or business processes) working within your organization might use the manage keys feature to create a key and use it to lock your environments in the tenant.*

## Prerequisites

- An Azure subscription that includes Azure Key Vault.
- Global tenant admin or an Azure AD with contributor permission to the Azure AD subscription and permission to create an Azure Key Vault and key. This is required to set up the key vault.
- Power Platform administrator must be assigned to either the Power Platform or Dynamics 365 Service administrator Azure AD role.



Enterprise policies (preview)

A policy is a pointer to an Azure resource (like Azure Key Vault). Policies can be added to multiple environments, as long as those environments are in the same region. Environments in different regions will need separate policies.

All policies | Environments with policies

| Name | Type | Azure region |
|---|---|---|
| PPEnterprisePolicy | Encryption | United States |

**Steps to configure** - the following steps link to detailed step by step documentation:

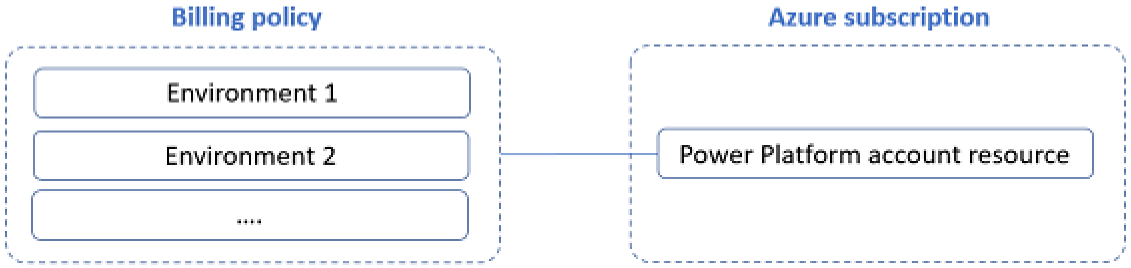
1. Create encryption key and grant access
2. Enable the Power Platform enterprise policies service for your Azure subscription
3. Create enterprise policy
4. Grant enterprise policy permissions to access key vault
5. Grant the Power Platform admin privilege to read enterprise policy
6. Add an environment to the enterprise policy to encrypt data

# Billing Policies

# What is a billing policy?

A billing policy creates a link between one or more environments and an Azure subscription. Used for PAYGO licensing models.

- It **consists** of:
  - Details of the **Azure subscription**
  - A **list of environments** that are **linked** to the **Azure subscription**
- Can be created in either **PPAC** or within Power Apps and Power Automate.
- When a policy is created, a corresponding Azure resource (called a **Power Platform account resource**) is created in the Azure subscription associated with that billing policy.
- Any **usage charges** for Power Apps, Power Automate, Dataverse, and Microsoft Power Platform requests will appear under the Power **Platform account resource** on the **Azure subscription's bill**.
- When an environment is linked to Azure via a billing policy, it becomes a **pay-as-you-go environment**.
  - An environment can only be linked to one billing policy at a time.
  - Environments can be removed from a policy at any time
    - It goes back to a regular environment.
  - *If a user has a premium per user license – it is used instead of PAYG*



Billing policy

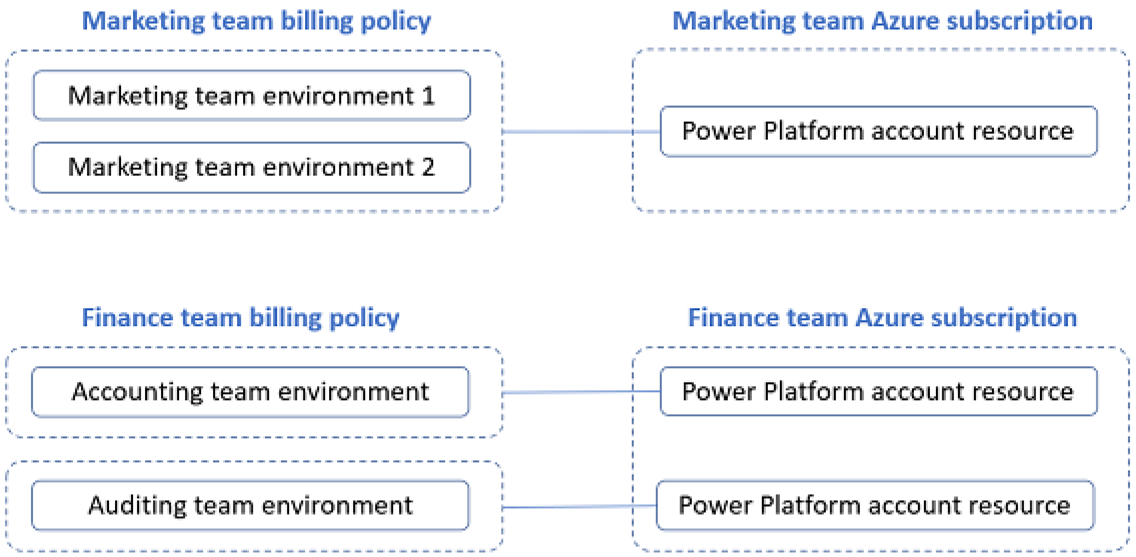
Environment 1

Environment 2

....

Azure subscription

Power Platform account resource



Marketing team billing policy

Marketing team environment 1

Marketing team environment 2

Marketing team Azure subscription

Power Platform account resource

Finance team billing policy

Accounting team environment

Auditing team environment

Finance team Azure subscription

Power Platform account resource

Power Platform account resource

# Setup billing policy/PAYGO

In order to set up pay-as-you-go billing for an environment, you first need an active Azure subscription that you can link to that environment. We recommend to configure this in PPAC.

**Who can set these up?**

- Power Platform Admin, Dynamics 365 Admin, Global Admin.
- Environment Admin – Can only link environments they are admins for and only to policies they create.

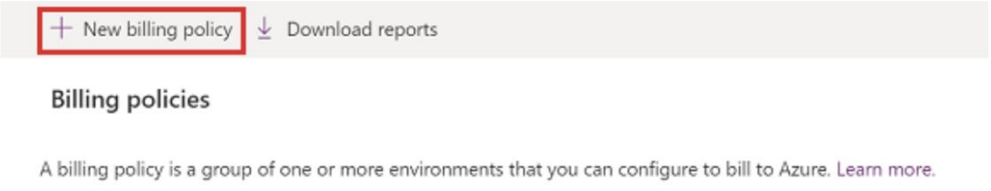
**Steps to configure**

1. First, procure or create an Azure subscription you can use
2. Navigate to Billing policies in PPAC and click **New Billing Policy**.
3. Provide a name for your new billing policy, and then select **Next**.
4. Add Azure subscription details
    1. Choose the **azure subscription** to bill from the drop-down list.
    2. Specify a **resource group** with that subscription.
    3. Specify a **region**
5. Select **Next**
6. Choose **environments to link** to the new billing policy.
7. Select one or more environments and click **Add to Policy**

    *Note: Only production or sandbox environments are available to add currently.*

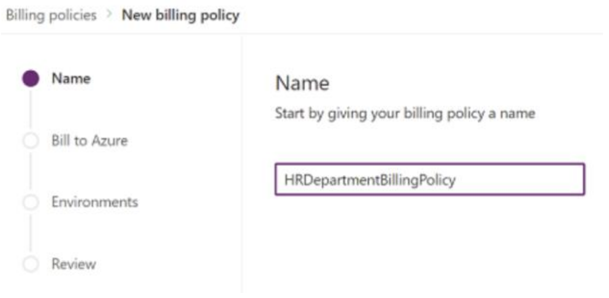
8. **Review** and **confirm**.

Optional: View the billing policy's Power Platform Account resource in the Azure Portal. Navigate to https://portal.azure.com/ > select the subscription > resource group > select view hidden types above resource list > You'll see a Power Platform account resource with the same name as the billing policy created.



Billing policies

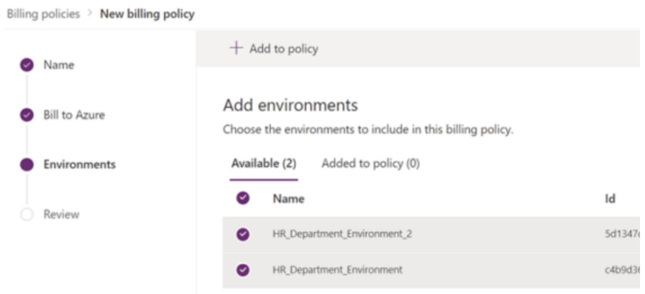
A billing policy is a group of one or more environments that you can configure to bill to Azure. Learn more.



Name

Start by giving your billing policy a name

HRDepartmentBillingPolicy

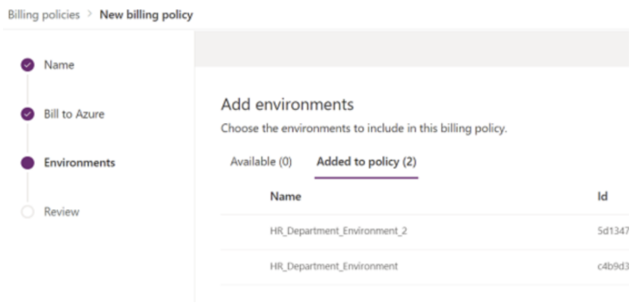


Add environments

Choose the environments to include in this billing policy.

Available (2) | Added to policy (0)

| Name | Id |
|---|---|
| HR_Department_Environment_2 | 5d1347( |
| HR_Department_Environment | c4b9d3( |

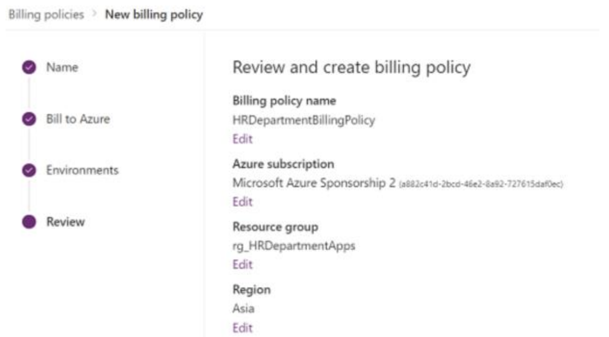


Add environments

Choose the environments to include in this billing policy.

Available (0) | Added to policy (2)

| Name | Id |
|---|---|
| HR_Department_Environment_2 | 5d1347 |
| HR_Department_Environment | c4b9d3 |



Review and create billing policy

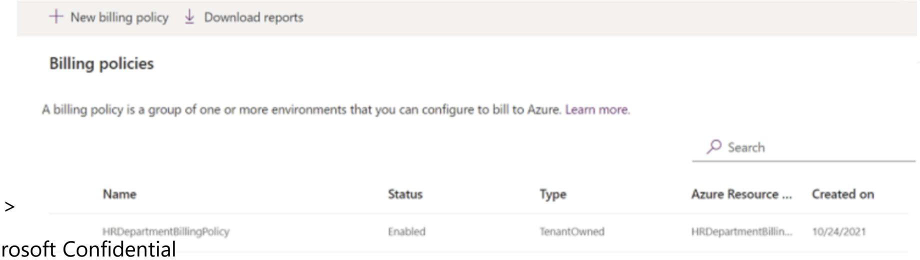
Billing policy name
HRDepartmentBillingPolicy
Edit

Azure subscription
Microsoft Azure Sponsorship 2 (a882c41d-2bcd-46e2-8a92-727615daf0ec)
Edit

Resource group
rg_HRDepartmentApps
Edit

Region
Asia
Edit

Environments
2 environment(s) selected
Edit



Billing policies

A billing policy is a group of one or more environments that you can configure to bill to Azure. Learn more.

| Name | Status | Type | Azure Resource ... | Created on |
|---|---|---|---|---|
| HRDepartmentBillingPolicy | Enabled | TenantOwned | HRDepartmentBillin... | 10/24/2021 |

# Questions?

# Lab 1 and 2

| Lab Description |
|---|
| **Lab 1. Create DLP Policy in Power Platform Admin Center**<br>**Lab 2. Create DLP Policy using PowerShell** |

Microsoft

© Copyright Microsoft Corporation. All rights reserved.