Microsoft

Workshop
Power Platform
for Administrators

Data Loss Prevention (DLP) Policies

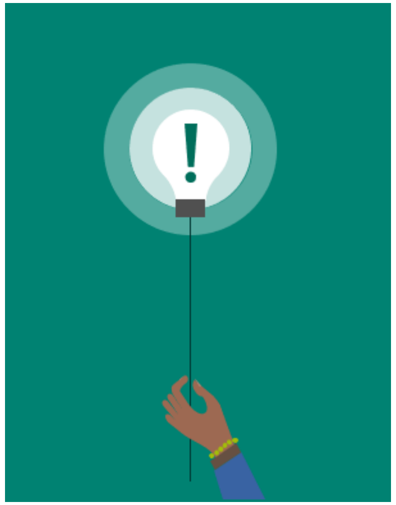
Learning Units covered in this Module

Understand Data Loss Prevention Policies

Objectives

After completing this module, you will learn:

- What Power Platform Data Loss Prevention policies are
- Who can create and manage policies
- How policies are enforced and visible to users
- What means granular DLP control and what granular options there are
- DLP management interfaces

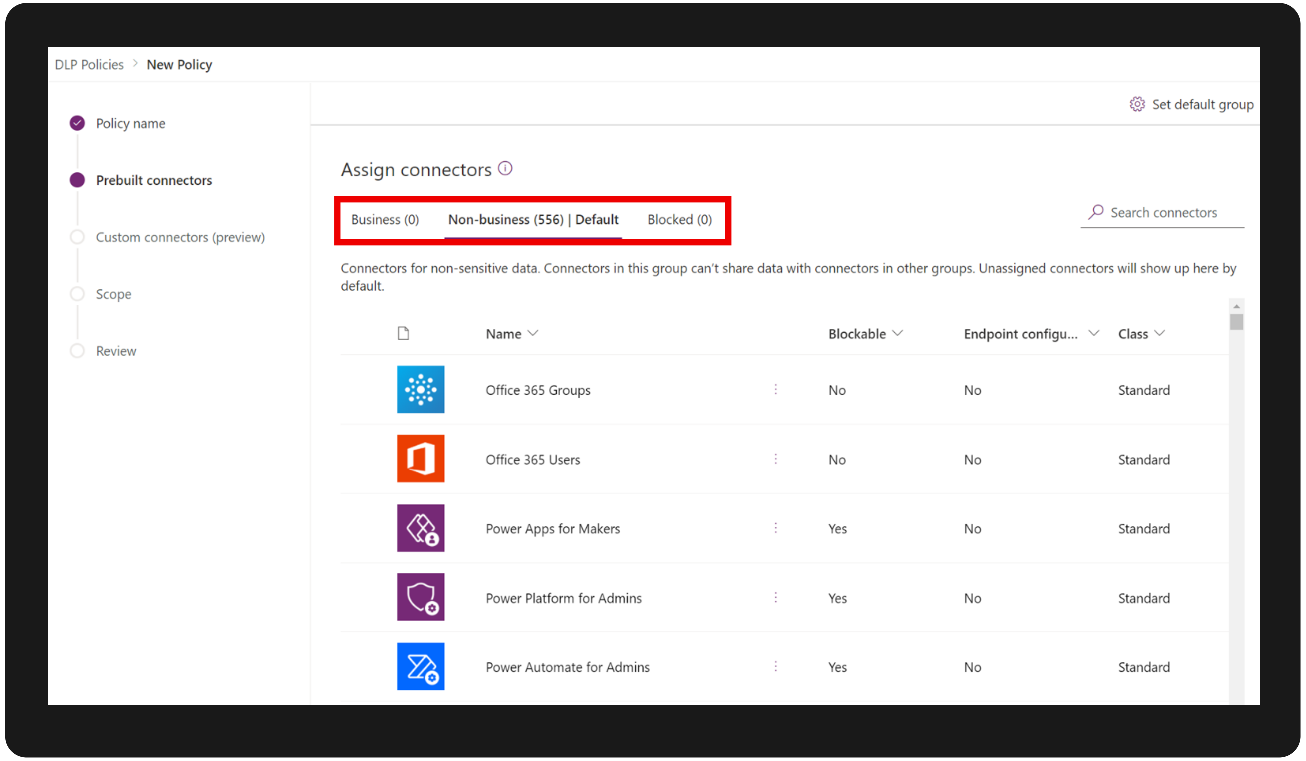


Understand Data Loss Prevention Policies

What are Data Loss Prevention (DLP) policies?

Sub-Heading

- 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.



DLP Policies > New Policy

- Policy name
- Prebuilt connectors
- Custom connectors (preview)
- Scope
- Review

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 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

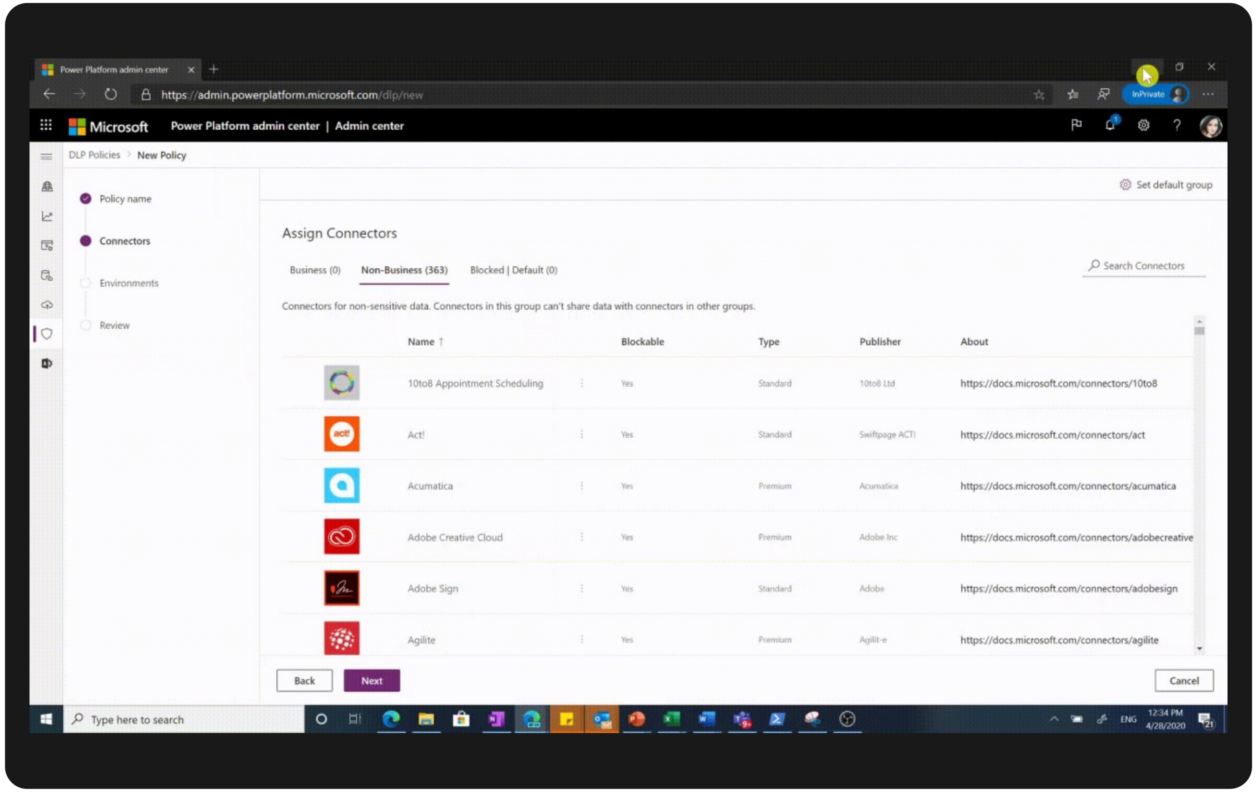
Blocked

- 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

Following grouping logic is applied to new connectors added to Power Platform:

- Power Platform connector ecosystem keeps evolving and adding new connectors
- If 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



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

Power Platform DLP allows admins to create two types of policies

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.

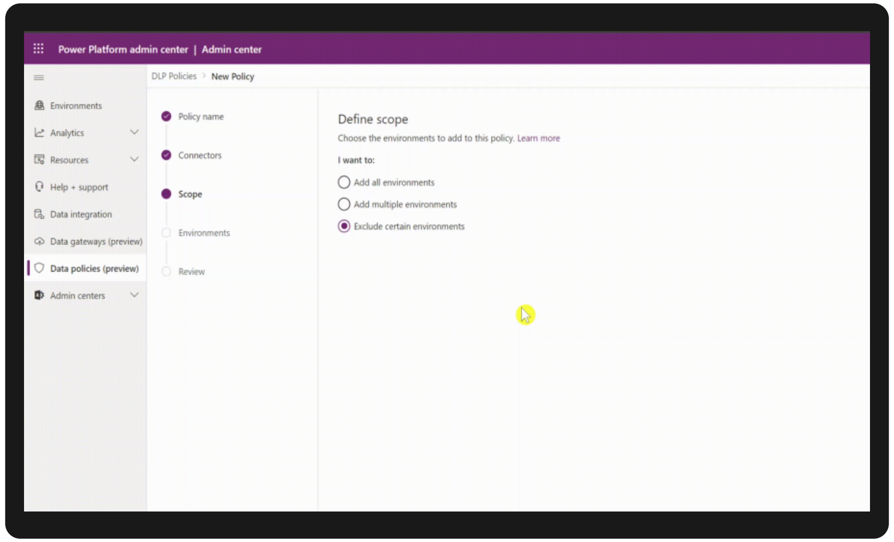
Only selected environments

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

Environment policies have one setting

One environment only

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



Define scope

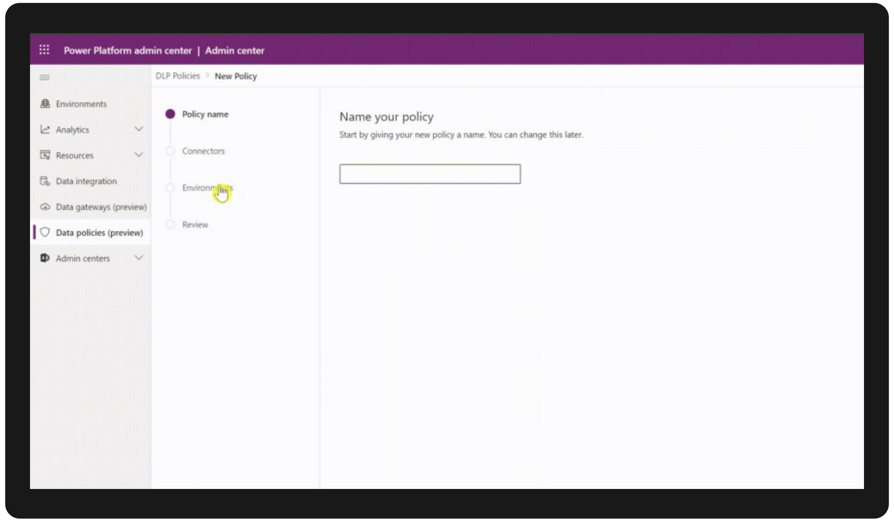
Choose the environments to add to this policy. Learn more

I want to:

○ Add all environments

○ Add multiple environments

● Exclude certain environments



Name your policy

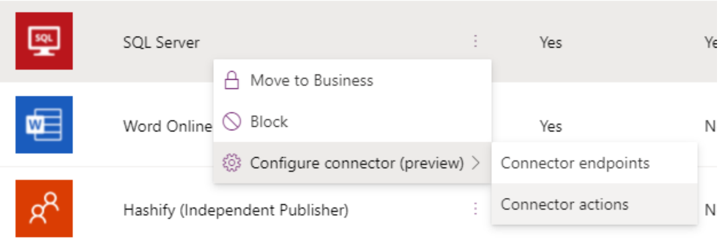
Start by giving your new policy a name. You can change this later.

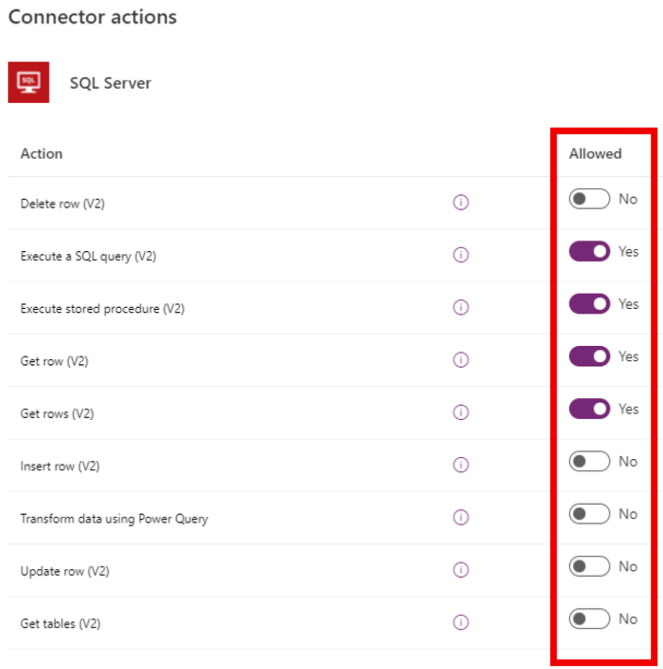
Connector Action Control

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

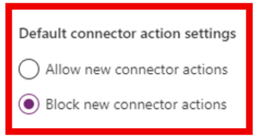




Connector actions

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

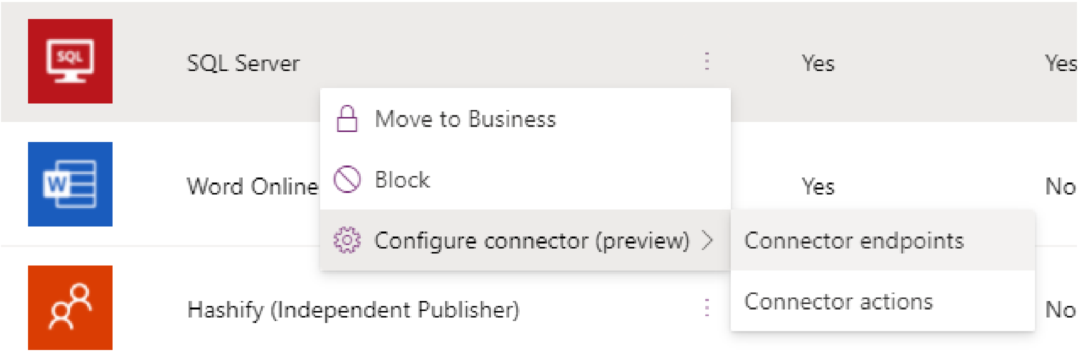
○ Allow new connector actions

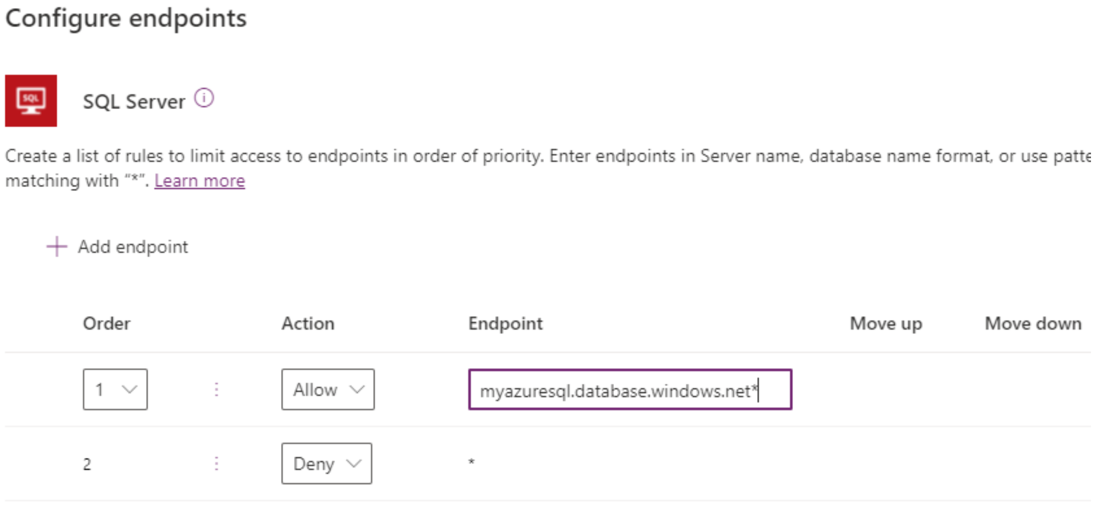
● Block new connector actions

Endpoint Filtering

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 facility 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 [here]()




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

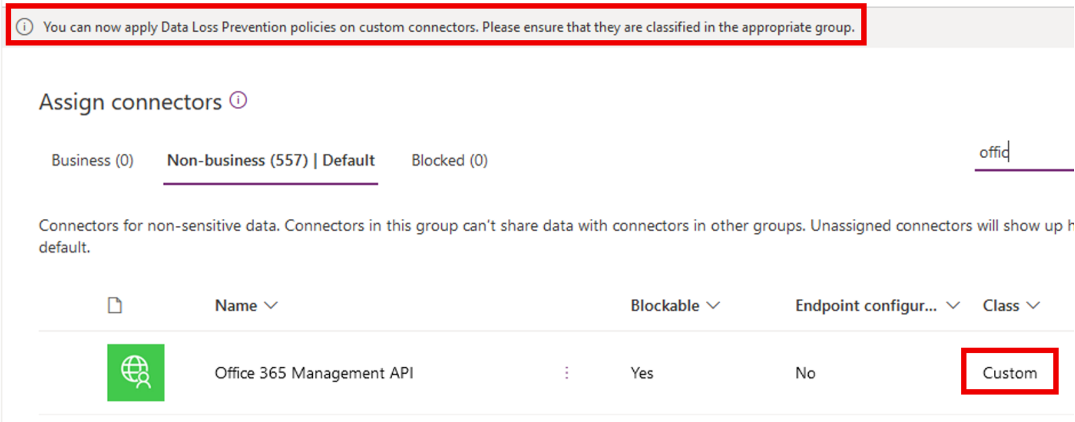
+ Add endpoint

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.

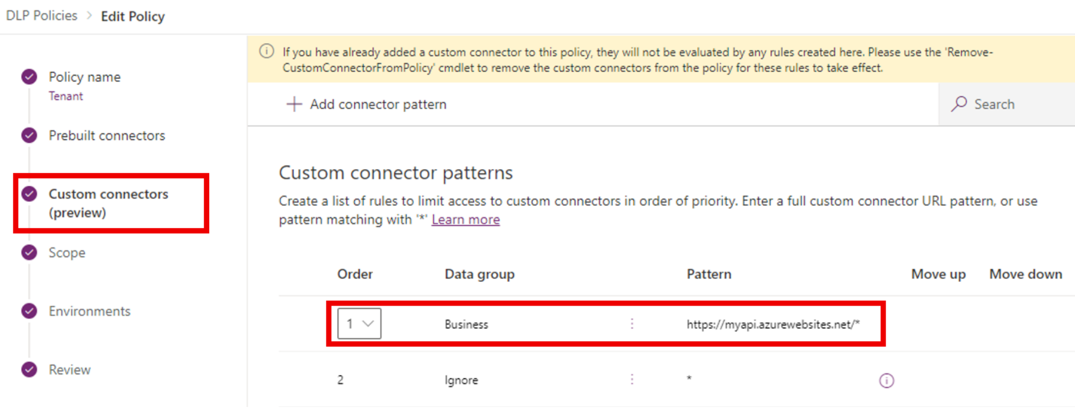


ⓘ You can now apply Data Loss Prevention policies on custom connectors. Please ensure that they are classified in the appropriate group.

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

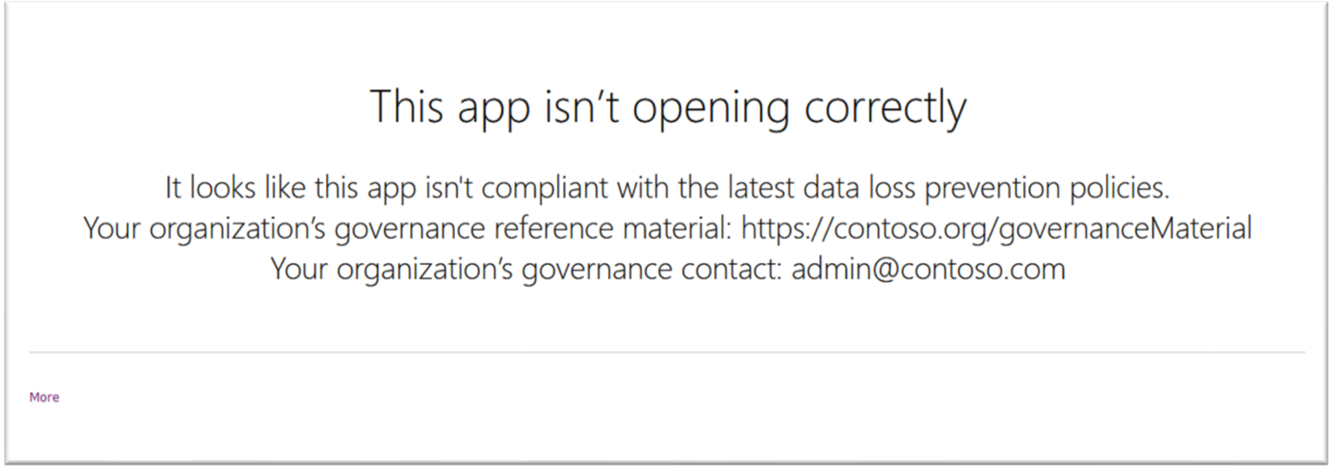
Create a list of rules to limit access to custom connectors in order of priority. Enter a full custom connector URL pattern, or use pattern matching with '*' Learn more

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

https://docs.microsoft.com/en-us/power-platform/admin/dlp-custom-connector-parity

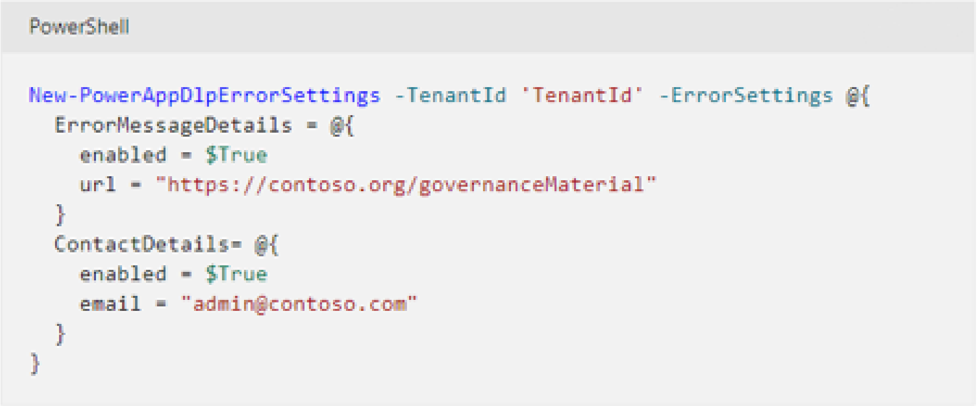
DLP Governance Error Message

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

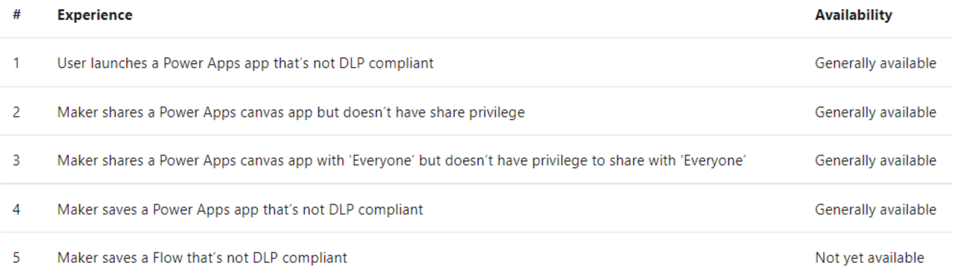


This app isn’t opening correctly

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



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

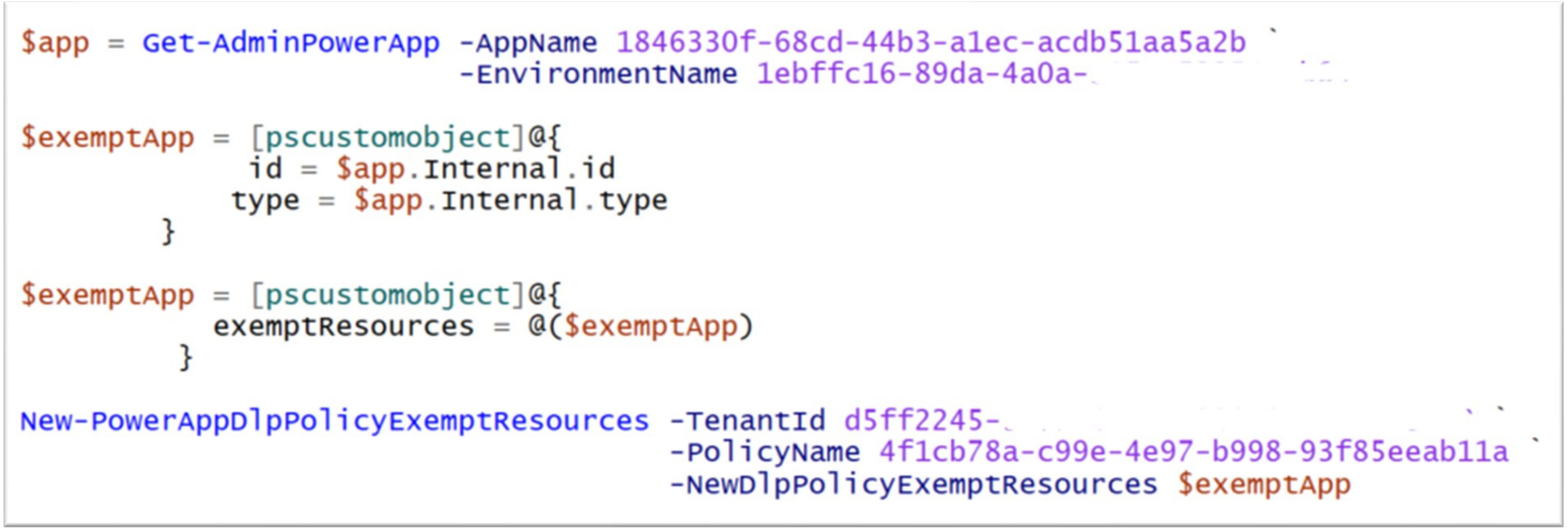


#	Experience	Availability
1	User launches a Power Apps app that’s not DLP compliant	Generally available
2	Maker shares a Power Apps canvas app but doesn’t have share privilege	Generally available
3	Maker shares a Power Apps canvas app with ‘Everyone’ but doesn’t have privilege to share with ‘Everyone’	Generally available
4	Maker saves a Power Apps app that’s not DLP compliant	Generally available
5	Maker saves a Flow that’s not DLP compliant	Not yet available

https://docs.microsoft.com/en-us/power-platform/admin/powerapps-powershell#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.



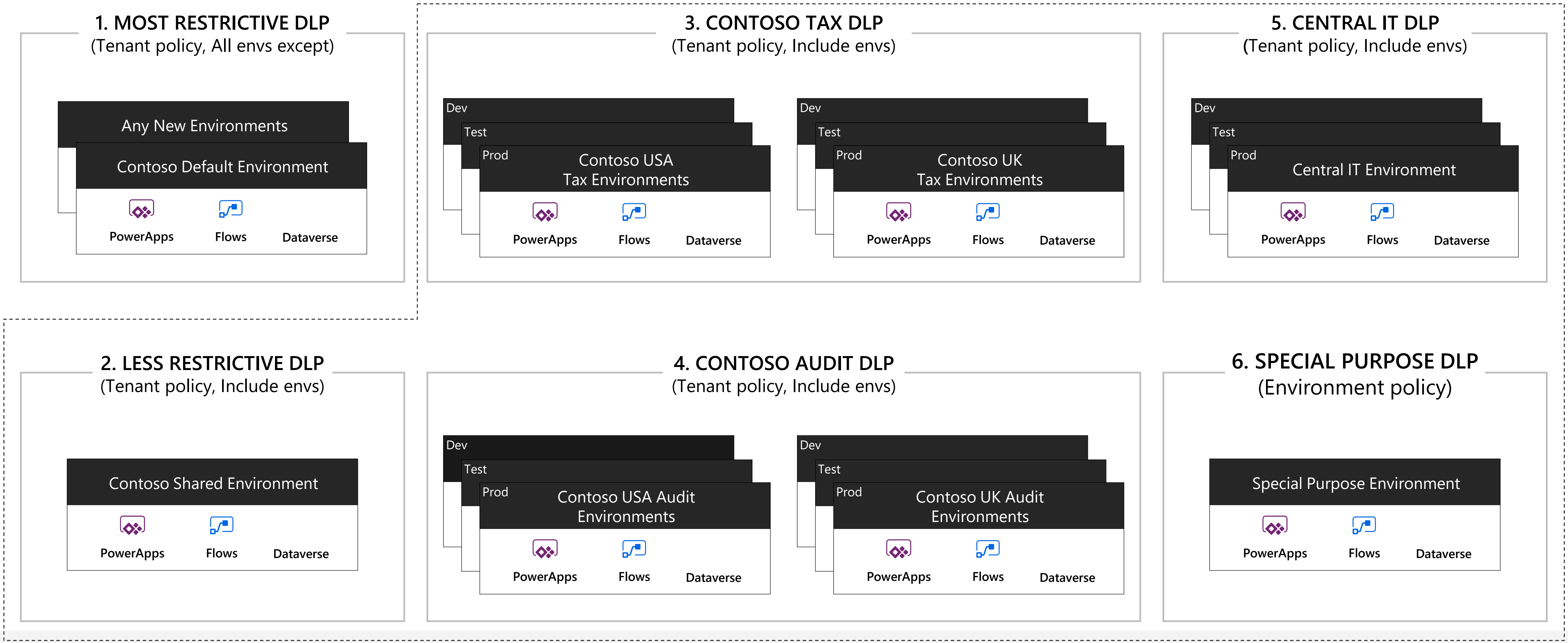
```
$app = Get-AdminPowerApp -AppName 1846330f-68cd-44b3-a1ec-acdb51aa5a2b `
                         -EnvironmentName 1ebffc16-89da-4a0a-[redacted]

$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
```

https://docs.microsoft.com/en-us/power-platform/admin/powerapps-powershell#dlp-resource-exemption-cmdlets

Demonstration

Create tenant level Data Loss Prevention 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

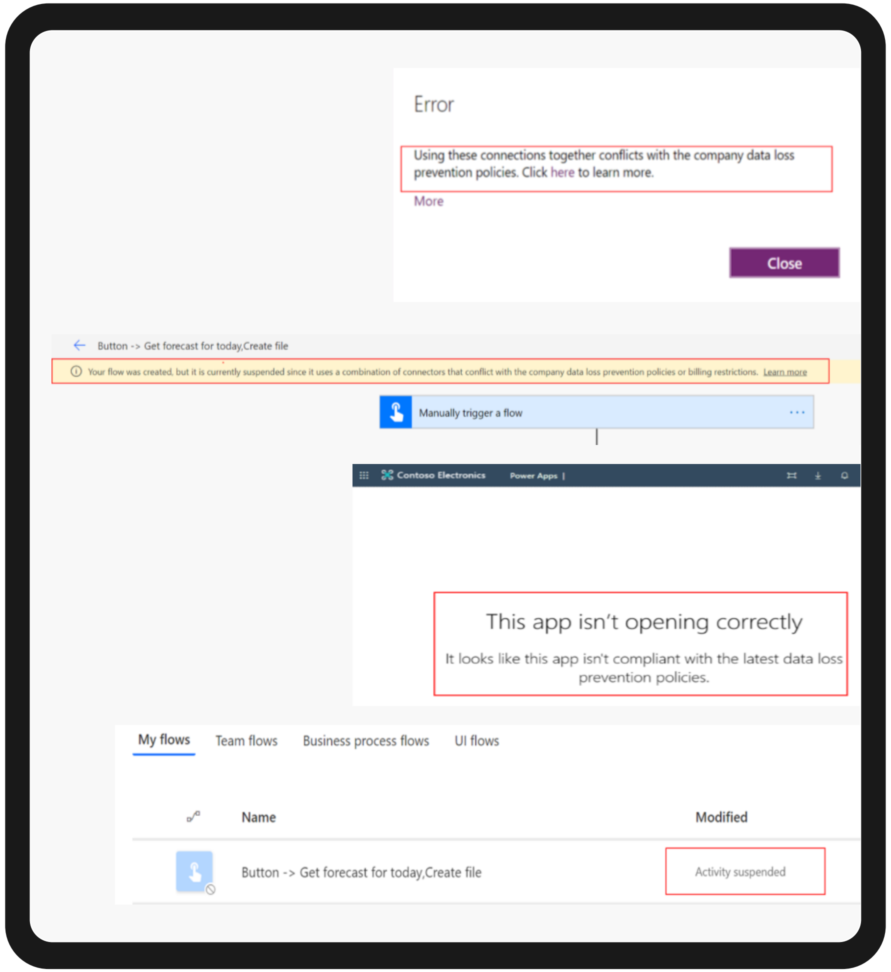
Power Platform DLP allows admins to create two types of policies

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. Flow will be saved but marked as 'Suspended' and will not execute unless DLP violation is resolved.

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.



Error

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

Button -> Get forecast for today,Create file

Your flow was created, but it is currently suspended since it uses a combination of connectors that conflict with the company data loss prevention policies or billing restrictions. 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

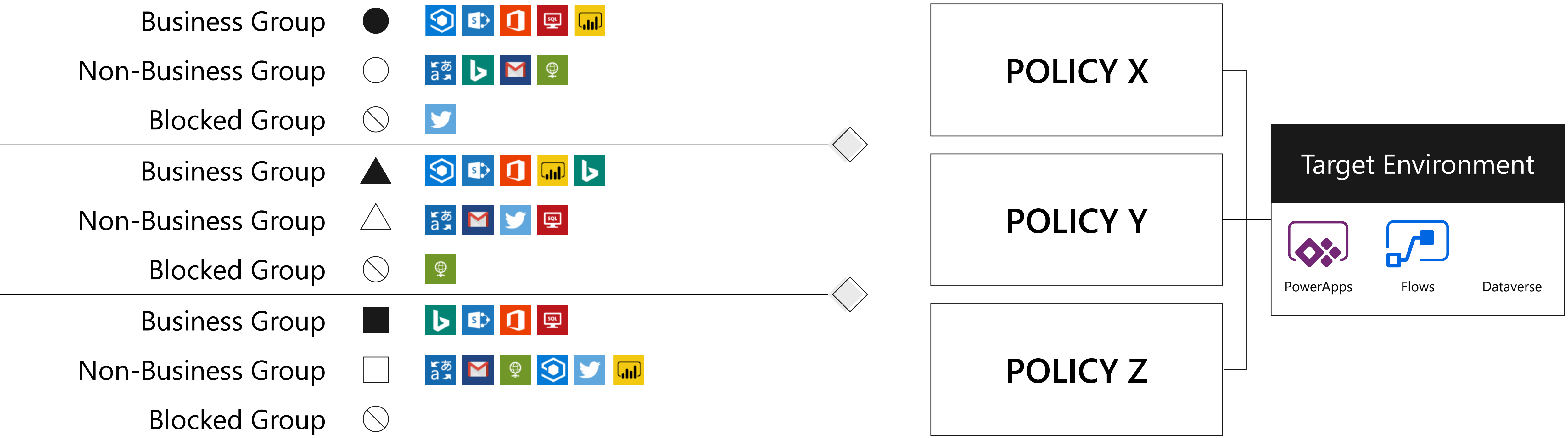
If all DLP policies applied to the environment mark a certain set of connectors as business or non-business, then the most restrictive groupings define what connectors can be used together vs. Not.

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

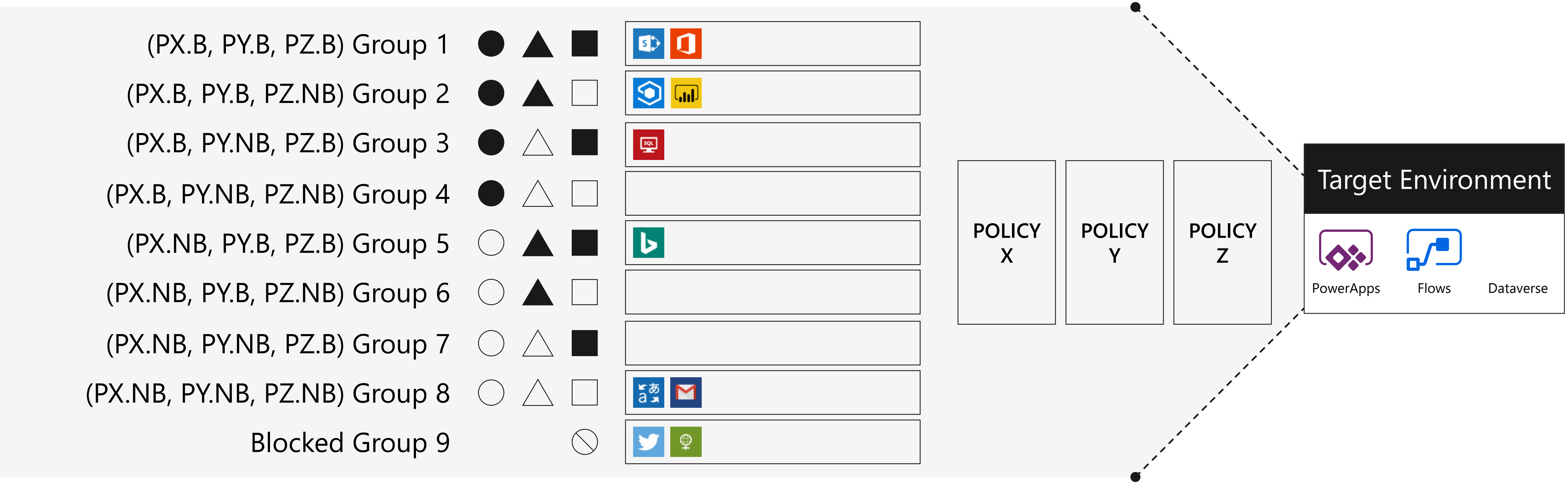
PowerApps

Flows

Dataverse

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 – <u>Fragmented and hard to predict</u>

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

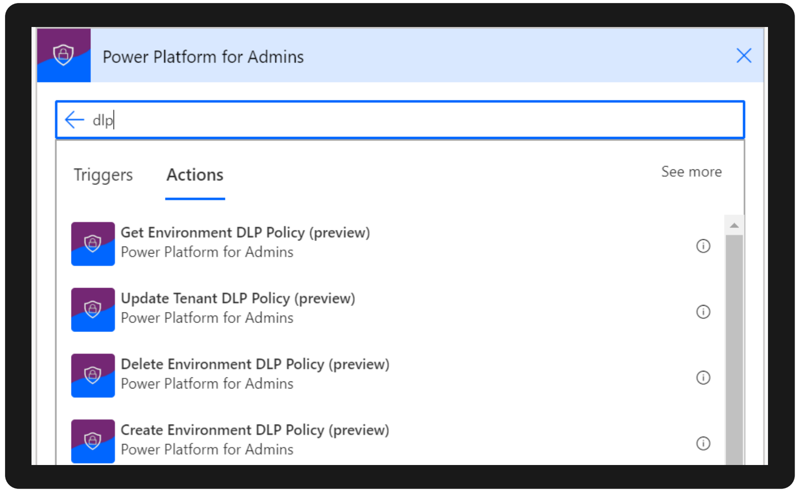
Flows

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



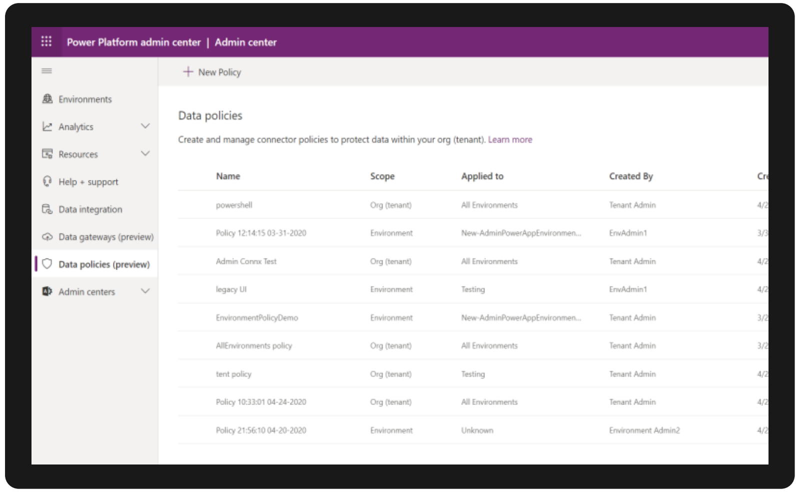
Get Environment DLP Policy (preview)
Power Platform for Admins

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

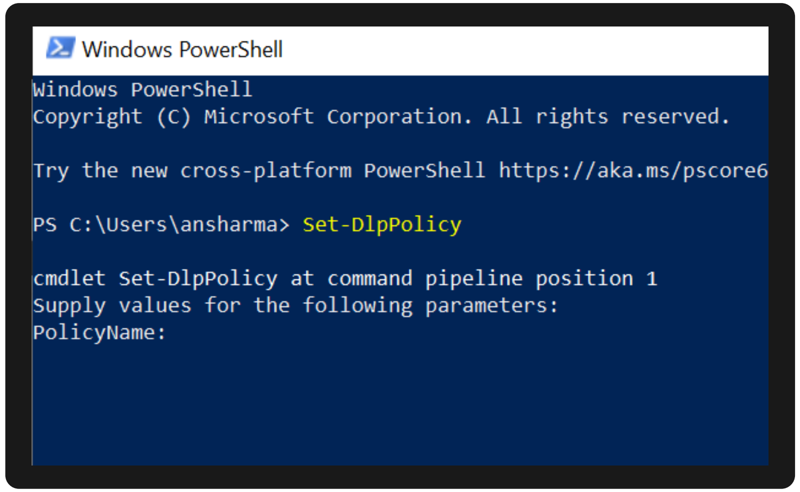


Data policies

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

Questions?

Create DLP Policy in Power Platform Admin Center

Create DLP Policy using PowerShell

Microsoft