

WorkshopPLUS

Power Platform for Admins

Module 4 – Power Platform DLP Policies

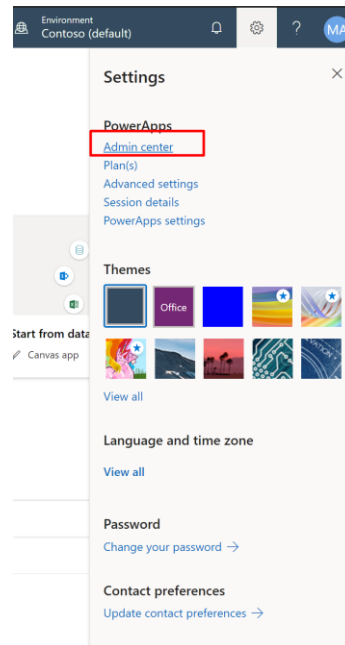
Content

Lab 1 - Create DLP Policy in Admin Center	2
Exercise 1 - Create DLP Policy for Contoso Environment	2
Lab 2 – Use PowerShell to manage DLP Policies.....	7
Exercise 1 - Creating a DLP policy using PowerShell.....	7
Exercise 2 - Add a custom connector to “Contoso Production” environment	9
Exercise 3 - Add custom connector to DLP policy.....	12

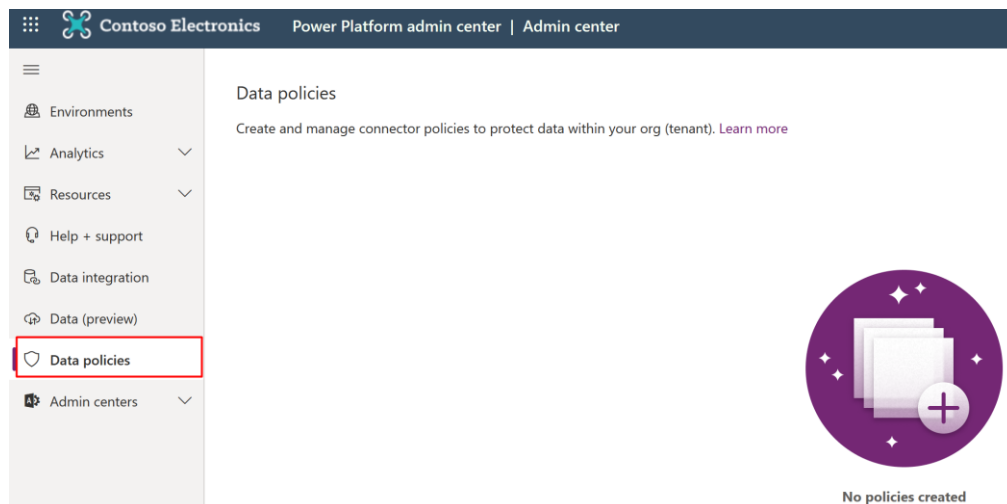
Lab 1 - Create DLP Policy in Admin Center

Exercise 1 - Create DLP Policy for Contoso Environment

1. In this exercise, you will use a global admin or Power Platform admin account to create DLP policies.
2. Using a tenant global admin, navigate to [www.aka.ms/ppac](https://aka.ms/ppac) or <https://admin.powerplatform.microsoft.com> or, from Power Apps studio, select the gear button on top right-hand side and choose **Admin center**, then select Environments.



3. At the left navigation pane, click on Data Polices, then click **+New Policy**.



4. At the policy name section, type “Default Environment Policy” then click Next.

Contoso Electronics Power Platform admin center | Admin center

DLP Policies > New Policy

Policy name

Connectors

Scope

Review

Name your policy

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

Default Environment Policy

5. At the connectors section, note that all connectors are listed in the Non-business default group. You can use “Set default group” to change to other data groups as shown below. Keep Non-business data group as default data group.

DLP Policies > New Policy

Policy name

Connectors

Scope

Review

Assign connectors

Business (0) Non-business (422) | Default Blocked (0)

Search 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 Class Publisher About

Set default group

Business
Connectors for sensitive data.

Non-business
Connectors for non-sensitive data.

Blocked
Blocked connectors can't be used where this policy is applied. (Unblockable connectors will be in Non-business by default.)

Apply Cancel

6. Search for the Twitter connector and block it

DLP Policies > New Policy

Policy name
Connectors
Scope
Review

Move to Business Block

Set default group

Assign connectors ⓘ

Business (0) Non-business (422) | Default Blocked (0)

Search 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	Class	Publisher	About
Twitter	Yes	Standard	Microsoft	Learn about Twitter

Move to Business
Block

7. Search for the following connectors to allow them in the Business group only: SharePoint – Office 365 Users – Office 365 Outlook, then click Next.

DLP Policies > New Policy

Policy name
Connectors
Scope
Review

Set default group

Assign connectors ⓘ

Business (3) Non-business (417) | Default Blocked (2)

Search connectors

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

Name ↑	Blockable	Class	Publisher	About
Office 365 Outlook	No	Standard	Microsoft	Learn about Office 365 Outlook
Office 365 Users	No	Standard	Microsoft	Learn about Office 365 Users
SharePoint	No	Standard	Microsoft	Learn about SharePoint

8. Define the policy scope by selecting “Add multiple environments”, then click Next.

DLP Policies > **New Policy**

✓ Policy name

✓ Connectors

Scope

○ Environments

○ Review

Define scope

Choose the environments to add to this policy. [Learn more](#)

I want to:

☐ Add all environments ⓘ

☒ Add multiple environments

☐ Exclude certain environments

9. Select the “Contoso (default)” environment then click “Add to policy” then click Next.

DLP Policies > **New Policy**

✓ Policy name

✓ Connectors

✓ Scope

Environments

○ Review

+ Add to policy

Add environments

Choose the environments to include in this policy. [Learn More](#)

Available (2)

Added to policy (0)

Name ↑	Id	Type	Region	Created by	Created
<input checked="" type="checkbox"/> Contoso (default)	Default-bac...	Default	unitedstates	SYSTEM	11/3/2020
Contoso Production	eba41d3d-0...	Trial	europe	MOD Administra...	11/16/2020

10. Review the policy setup then click Create policy.

DLP Policies > New Policy

✓ Policy name

✓ Connectors

✓ Scope

✓ Environments

● Review

Review and create policy

Policy name

Default Environment Policy

Edit

Connectors

(3) Business, (417) Non-business, (2) Blocked

Edit

Scope

Add multiple environments

Edit

Environments

1 environment(s) selected

Edit

✓ The policy was successfully deleted.

Data policies

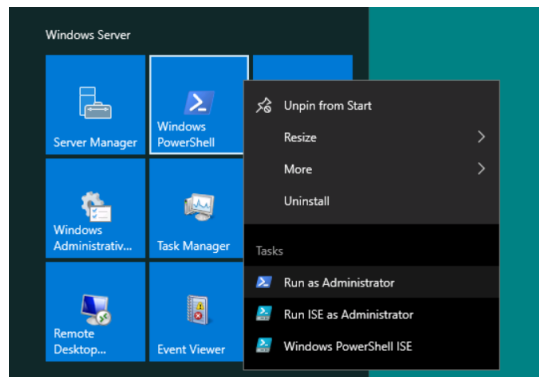
Create and manage connector policies to protect data within your org (tenant). [Learn more](#)

Name	Scope	Applied to	Created by	Created
Default Environment Policy	Org (tenant)	Contoso (default)	MOD Administrator	11/18/2020

Lab 2 – Use PowerShell to manage DLP Policies

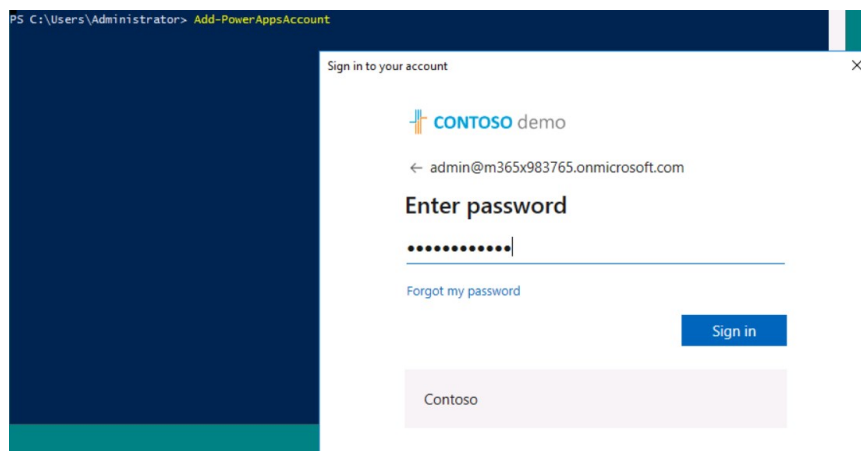
Exercise 1 - Creating a DLP policy using PowerShell

1. Run Windows PowerShell as an administrator.



2. Force PowerShell cmdlet to use TLS 1.2 by running the following command
`[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12`
3. Install Power Apps administration PowerShell.
`Install-Module -Name Microsoft.PowerApps.Administration.PowerShell -Force`
4. Add Power Platform Admin account (global admin) by running the command below
`Add-PowerAppsAccount`

This command will prompt a window requiring you to enter a username and password, use the global admin credentials then sign-in.



5. Get Contoso Production environment by display name.

```
$selectedEnvironment = Get-AdminPowerAppEnvironment "Contoso Production"
```

6. Create a new DLP policy for Contoso Production only.

```
$newPolicy = New-AdminDlpPolicy -DisplayName "Contoso Production Policy" -  
EnvironmentName $selectedEnvironment.EnvironmentName
```

7. Type \$newPolicy variable which stores created policy details.

```
PS C:\WINDOWS\system32> Add-PowerAppsAccount
PS C:\WINDOWS\system32> $selectedEnvironment = Get-AdminPowerAppEnvironment "Contoso Production"
PS C:\WINDOWS\system32> $newPolicy = New-AdminDlpPolicy -DisplayName "Contoso Production Policy" -EnvironmentName $selectedEnvironment.EnvironmentName
PS C:\WINDOWS\system32> $newPolicy

PolicyName      : ae725ce6-e83f-4781-bd6e-6f3d70056694
Type            : Microsoft.BusinessAppPlatform/scopes/environments/apiPolicies
DisplayName     : Contoso Production Policy
CreatedTime     : 2021-01-13T15:57:49.8096454Z
CreatedBy       : @{id=e9f33527-915b-48d8-8e35-19eea7eee91e; displayName=MOD Administrator; email=admin@M365x141415.0nMicrosoft.com; type=User; tenantId=bacb29a2-896b-4d06-bf77-d896601ebe75; userPrincipalName=admin@M365x141415.onmicrosoft.com}
LastModifiedTime : 2021-01-13T15:57:49.8096454Z
LastModifiedBy  : @{id=e9f33527-915b-48d8-8e35-19eea7eee91e; displayName=MOD Administrator; email=admin@M365x141415.0nMicrosoft.com; type=User; tenantId=bacb29a2-896b-4d06-bf77-d896601ebe75; userPrincipalName=admin@M365x141415.onmicrosoft.com}
Constraints     : @{environmentFilter1=}
BusinessDataGroup : {}
NonBusinessDataGroup : {}
BlockedGroup    :
FilterType      : include
Environments     : @{name=d56a2895-47ec-4e96-9dfc-3d1919fd2ebf; id=/providers/Microsoft.BusinessAppPlatform/scopes/admin/environments/d56a2895-47ec-4e96-9dfc-3d1919fd2ebf; type=Microsoft.BusinessAppPlatform/scopes/environments}}
```

DLP Policies > Edit Policy

Policy name
Contoso Production Policy

Connectors

Environments

Review

Add an environment

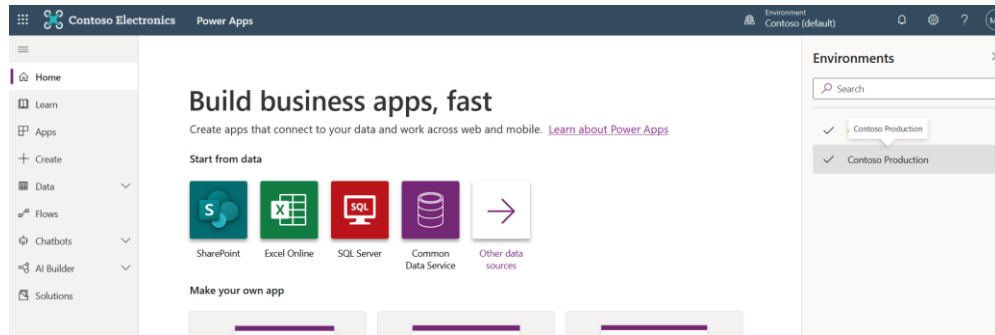
Choose an environment to include in this policy. Environment admins can only create policies for one environment at a time. [Learn More](#)

Available (1) **Added to policy (1)**

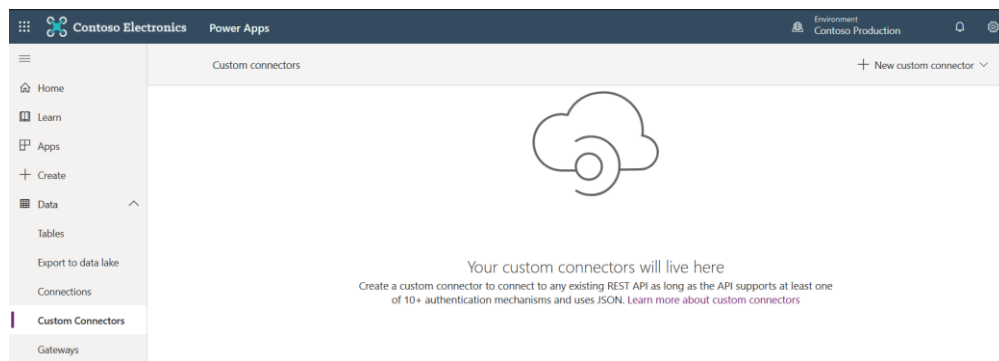
Name ↑	Id	Type	Region	Created by
Contoso Production	d56a2895-4...	Trial	europe	MOD Administra...

Exercise 2 - Add a custom connector to “Contoso Production” environment

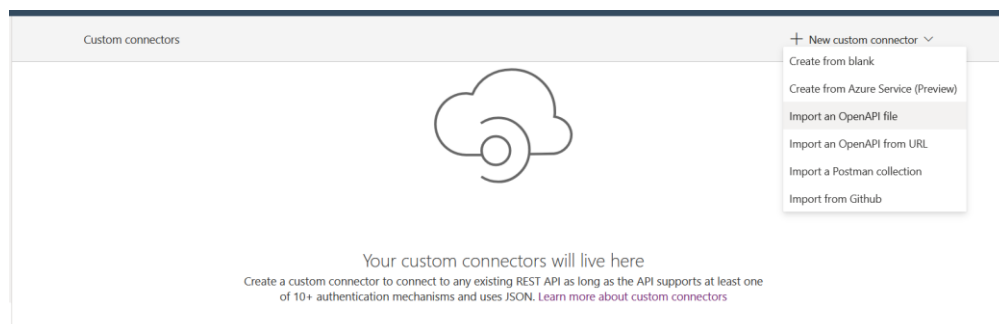
1. Navigate to <http://make.powerapps.com>
2. Switch the environment selector to use “Contoso Production” environment.



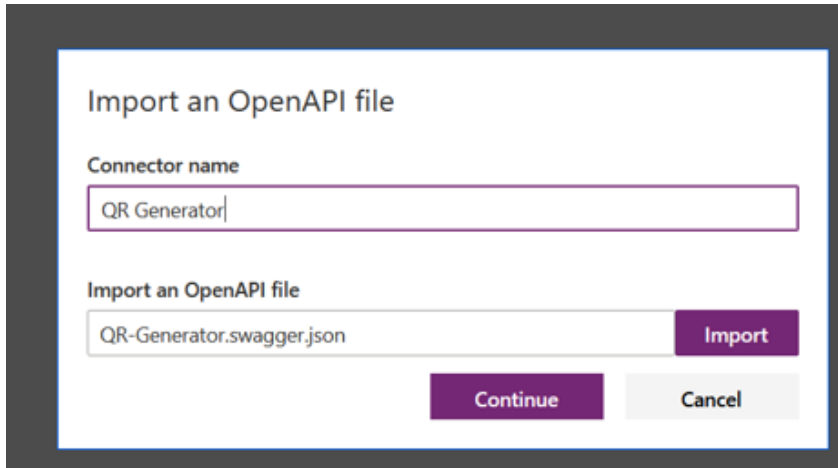
3. At the left navigation panel, select Data tab then select “Custom Connectors”



4. Click on “New custom connector” then select “Import an OpenAPI file”

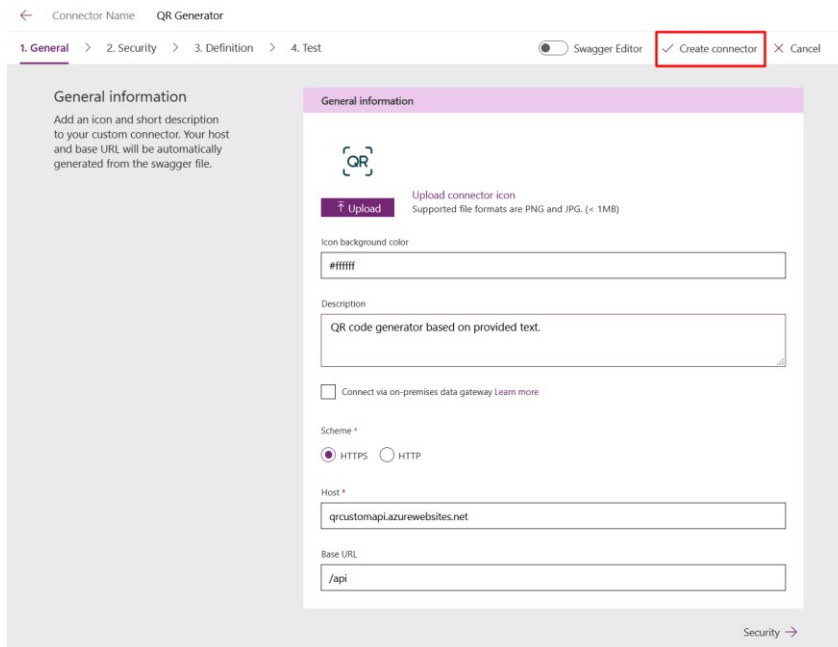


5. Type the connector name “QR Generator” then import the OpenAPI file from lab files named “QR-Generator.swagger.json” then click Continue



The screenshot shows a dialog box titled "Import an OpenAPI file". It has a text input field for "Connector name" containing "QR Generator". Below it is another text input field for "Import an OpenAPI file" containing "QR-Generator.swagger.json". To the right of this field is a purple "Import" button. At the bottom of the dialog are two buttons: a purple "Continue" button and a grey "Cancel" button.

6. Custom connector will import the file and navigate to the general information page, add the following information:
 - Upload the icon image from lab files named “customconnectoricon.png”
 - Icon background color #ffffff
 - Description: QR code generator based on provided text.
7. Leave rest of the settings, then click on Create Connector, then click Close.



The screenshot shows the "General information" page for a connector named "QR Generator". The page has a breadcrumb trail: "Connector Name > QR Generator". Below the breadcrumb is a tabbed interface with tabs for "1. General", "2. Security", "3. Definition", and "4. Test". The "1. General" tab is active. On the right side of the tab, there are three buttons: "Swagger Editor" (disabled), "Create connector" (highlighted with a red box), and "Cancel". The main content area is titled "General information" and contains the following fields:

- "Upload connector icon" with an "Upload" button and text: "Supported file formats are PNG and JPG. (< 1MB)".
- "Icon background color" with a text input field containing "#ffffff".
- "Description" with a text input field containing "QR code generator based on provided text.".
- A checkbox labeled "Connect via on-premises data gateway Learn more" which is unchecked.
- "Scheme" with radio buttons for "HTTPS" (selected) and "HTTP".
- "Host" with a text input field containing "qrcustomapi.azurewebsites.net".
- "Base URL" with a text input field containing "/api".

At the bottom right of the page is a "Security" link with a right-pointing arrow.

8. Created connector should be displayed in custom connectors list as shown below

Custom connectors		+ New custom connector ▾			
Name					
	QR Generator MOD Administrator	+	↓		...

NOTE that new added custom connector is not showing in the created policy for Contoso Production environment, you will add this custom connector in next lab exercise.

Exercise 3 - Add custom connector to DLP policy

1. Create a variable to store custom connector details.
\$customConnector = Get-AdminPowerAppConnector -ConnectorName "QR Generator"
2. Add the following command to add created custom connector to the policy.
Add-CustomConnectorToPolicy -PolicyName \$newPolicy.PolicyName -EnvironmentName \$selectedEnvironment.EnvironmentName -ConnectorName \$customConnector.ConnectorName -ConnectorId \$customConnector.ConnectorId -GroupName "hbi" -ConnectorType "Microsoft.PowerApps/apis"
3. Run command below to see that custom connector has been added to BusinessDataGroup of the policy

Get-AdminDlpPolicy -PolicyName \$newPolicy.PolicyName

```
PS C:\Users\Administrator> Get-AdminDlpPolicy -PolicyName $newPolicy.PolicyName

PolicyName      : 5291988c-55f6-4ba4-bd5d-638fb9240bff
Type            : Microsoft.BusinessAppPlatform/scopes/environments/apiPolicies
DisplayName     : Contoso Production Policy
CreatedTime     : 2021-02-19T07:50:30.8413218Z
CreatedBy      : @{{id=962d290d-f9bf-4eb8-b822-2aba58281876; displayName=MOD Administrator; email=admin@M365x737698.OnMicrosoft.com; type=User; tenantId=081d828c-92d4-4926-b2cc-8d073e4fb13b; userPrincipalName=admin@M365x737698.onmicrosoft.com}}
LastModifiedTime : 2021-02-19T07:55:21.6156758Z
LastModifiedBy  : @{{id=962d290d-f9bf-4eb8-b822-2aba58281876; displayName=MOD Administrator; email=admin@M365x737698.OnMicrosoft.com; type=User; tenantId=081d828c-92d4-4926-b2cc-8d073e4fb13b; userPrincipalName=admin@M365x737698.onmicrosoft.com}}
Constraints     : @{{environmentFilter=}}
BusinessDataGroup : {{id=/providers/Microsoft.PowerApps/apis/shared_qr-20generator-5f0620d66b78848c2a-5f69b32f757; name=shared_qr-20generator-5f0620d66b78848c2a-5f69b3e80b8282f757; type=Microsoft.PowerApps/apis}}
NonBusinessDataGroup : {}
BlockedGroup    :
FilterType      : include
Environments    : {{name=53e17125-9c12-4a9c-93d0-7122bf63d327; id=/providers/Microsoft.BusinessAppPlatform/admin/environments/53e17125-9c12-4a9c-93d0-7122bf63d327; type=Microsoft.BusinessAppPlatform/scopes/environments}}
```

NOTE:

- Add-CustomConnectorToPolicy command will be deprecated and replaced with New-DlpPolicy, Set-DlpPolicy, Get-DlpPolicy and Remove-DlpPolicy commands which can be used to managed DLP connectors
- hbi is the code for Business group
- currently custom connectors are not showing in policy UI, if you try to run last command again, you will get an error message: Add-CustomConnectorToPolicy : The given connector is already present in the hbi group.