Frederick Pearson

fpearson@cloudstrucc.com

Configuration Guide

dataverse data loss prevention (DLP), Tenant isolation, and ‘lockbox’ tenant wide policy configuration

Pre-Requisites

* **User must have the Global Administrator Role assigned**

Purpose

The PowerPlatform includes hundreds of first- and third-party connectors allowing developers and configurators to integrate with other services using PowerAutomate Flow and custom connectors (for custom API’s). You can adopt a zero-trust policy in your organization, and the PowerPlatform by leveraging the Data Policies feature. It is recommended to block all third-party connectors in your PowerPlatform subscription and only allow connectors via your change management process (ticketing system). The PowerPlatform not only provides the ability to block or allow connectors ‘tenant-wide’ but also allow your organization’s client (or specific environments) seek exemptions for their use case.

Configure Tenant Wide DLP

Navigate to the [PowerPlatform Admin Centre](https://admin.powerplatform.microsoft.com/) and select Policies from the side menu and press “New Policy” ([directly link](tps://admin.powerplatform.microsoft.com/dlp/new))

Graphical user interface, application, Teams

Description automatically generated

Set the policy name to “Global (Tenant)” (or similar).

IN the Prebuild connectors menu, select the “nonbusiness” tab and filter the publisher column to “Microsoft” and press Apply. For a more restrictive list, see Annex A.

Graphical user interface, application

Description automatically generated

Once filtered, select all and press “Move to Business”

Graphical user interface, application, Teams

Description automatically generated

Next press “Clear all filters”. Select all connectors and press “Block” (this will block all third-party connectors).

Graphical user interface, application, Teams

Description automatically generated

Press next, leave Custom connectors set values as default, press next and make sure that Add all environments is checked

Graphical user interface, application

Description automatically generated

Press “Create Policy”

Graphical user interface, application

Description automatically generated

\*SECTION TO BE COMPLETED IN JUNE 2022\*

Configure Environment Specific DLP

You can configure DLP exemptions by creating a new policy that allows a connector(s). (TODO)

Configure Tenant Isolation (Preview)

*Should not be implemented in a production environment (until late 2022 or when in general availability)*

Configure Lockbox Policy (Preview)

*Should not be implemented in a production environment (until late 2022 or when in general availability)*

Configure Customer Lockbox Policy (Preview)

*Should not be implemented in a production environment (until late 2022 or when in general availability)*

Annex A: DLP Minimum Business Connectors

If you’re organization would like to restrict everything including Microsoft connectors, the following connectors could be part of the Business group while everything else is blocked by default. These will allow your organization to build and maintain integrations safely without losing key features the platform offers.

|  |  |
| --- | --- |
| Connector | Justification |
| Approvals | Required for CoE Kit |
| HTTP | Required for CoE Kit |
| HTTP with Azure AD | Required for CoE Kit |
| Microsoft Dataverse | Required for CoE Kit |
| Microsoft Dataverse (legacy) | Required for CoE Kit |
| Microsoft Teams | Required for CoE Kit |
| Office 365 Groups | Required for CoE Kit |
| Office 365 Outlook | Required for CoE Kit |
| Office 365 Users | Required for CoE Kit |
| Power Apps for Admins | Required for CoE Kit |
| Power Apps for Makers | Required for CoE Kit |
| Power Automate for Admins | Required for CoE Kit |
| Power Automate Management | Required for CoE Kit |
| Power Platform for Admins | Required for CoE Kit |
| RSS | Required for CoE Kit |
| SharePoint | Required for CoE Kit |
| OneDrive for Business | Required for transitory docs (if required in future requirement) – restricted to tenant only (by default)) |
| OneDrive | Required for transitory docs (if required in future requirement) – restricted to tenant hosted one drive only (by default)) |
| SQL Server |  |
| Dynamics 365 Sales Insights | PowerBI / General Reporting & Cross environment connections |
| Dynamics 365 Customer Insights | PowerBI / General Reporting & Cross environment connections |
| Power Query Dataflows | PowerBI / General Reporting & Cross environment connections |
| Fin and Ops Apps (Dynamics 365) | PowerBI / General Reporting & Cross environment connections |
| Excel | Reporting and Data administration |
| Excel Online (OneDrive) | Reporting and Data administration |
| Excel Online (Business) | Reporting and Data administration |
| Notifications | Teams notifications (for CRM/Teams integration) |
| Form Recognizer | Useful for hand filed forms (to support accessibility, paper based processes, and advanced scanning + printing official hard copy records) |
| Microsoft 365 Compliance | SIEM, Monitoring |
| Microsoft 365 Apps Health | SIEM, Monitoring |
| Dynamics 365 Customer Voice | Customer Voice (calling, contact us, support) |
| Microsoft Graph Security | General API usage for Azure |
| PowerApps Notifications | Used for configuring notifications within the PowerApps applications |
| PowerApps Notifications V2 | Used for configuring notifications within the PowerApps applications (additional features) |
| Power Virtual Agents | Client engagement (direct messaging & voice) |
| Service Bus | Used for messaging queues |
| PowerBI | Reporting |
| Azure KeyVault | Protection of certs and keys for Dataverse apps & ALM (DevOps) |
| Azure AD | Authorization / RBAC |
| Azure AD Identity Protection | Authorization / RBAC integration (e.g. AAD groups integration with D365) |
| Azure App Service | Used for hosting static sites and apps to support requirements |
| Azure Blob Storage | Leveraged for diagnostics, web file hosting, and system attachments |
| Azure Log Analytics | SIEM/Health Monitoring |