Microsoft Power Platform

M365 Minimum Viable Secure Configuration Baseline

Draft Version 0.1

October 2022
Cybersecurity and Infrastructure Security Agency
Secure Cloud Business Applications (SCuBA)

Record of Changes

No.	Date	Reference	A=Add
			M=Modify
			D=Delete
				Description of Change

v0.1	17 October 2022	Entire document	M	Initial Draft w/Edit

Table of Contents

1 Introduction 1

1.1 Assumptions 1

1.2 Resources 1

2 Baseline 1

2.1 Creation of Power Platform Environments SHALL Be Restricted 2

2.2 Data Loss Prevention Policies for Power Platform Environments SHALL Be Created 2

2.3 Tenant Isolation SHALL Be Enabled to Prevent Cross Tenant Access of Power Platform environments 4

2.4 Content Security Policy SHALL Be Enabled 5

3 Acknowledgements 6

List of Tables

Table 1. Connectors that can’t be blocked and must be moved to either Business/Non-Business Categories .... **Error! Bookmark not defined.**

This page is intentionally blank.

1 Introduction

The Microsoft Power Platform is a group of applications involving low-code application development, business intelligence, a custom chat bot creator, and app connectivity software. The following summarizes the Power Platform applications and other applications frequently used by Power Platform applications.

Power Apps: This is a low-code application development software used to create custom business applications. The apps can be used as desktop, mobile, and web apps. Three different types of Power Apps can be created:

1. **Canvas Apps**: These are drag and drop style developed apps, where users drag and add User Interface (UI) components to the screen. Users can then connect the components to data sources to display data in the canvas app.
2. **Model-Driven Apps**: These apps are developed from an existing data source. They can be thought of as the inverse of a Canvas App. For those familiar with the Model-View-Controller design pattern, Model-Driven apps revolve around building the view and controller on top of the model.
3. **Portals**: These apps are created to be websites.

Power Automate: This is an online tool within the Microsoft 365 (M365) applications and add-ins used to create automated workflows between apps and services to synchronize files, get notifications and collect data.

Power Virtual Agents: These are custom chat bots for use in the stand-alone Power Virtual Agents web app or in a Microsoft Teams channel.

Connectors: These are a proxy or a wrapper around an API that allows the underlying service to be accessed from Power Automate workflows, a Power App, or Azure Logic Apps.

Microsoft Dataverse: This is a cloud database management system most often used to store data in SQL-like tables. A Power App would then use a connector to connect to the Dataverse table and perform create, read, update, and delete (CRUD) operations.

1.1 Assumptions

The **License Requirements** sections of this document assume the organization is using an M365 E3 or G3 license level. Therefore, only licenses not included in E3/G3 are listed.

1.2 Resources

License Compliance and Copyright

Portions of this document are adapted from documents in Microsoft's M365 and Azure GitHub repositories. The respective documents are subject to copyright and are adapted under the terms of the Creative Commons Attribution 4.0 International license. Source documents that are linked throughout this document. The United States Government has adapted selections of these documents to develop innovative and scalable configuration standards to strengthen the security of widely used cloud-based software services.

2 Baseline

Baselines in this section are for administrative controls that apply to all Power Platform applications at the Power Platform tenant and environment level. Additional Power Platform security settings would be implemented at the app level, connector level, or Dataverse table level. Refer to Microsoft documentation for those additional controls.

2.1 Creation of Power Platform Environments SHALL Be Restricted

Power Platform environments are used to group, manage, and store Power Apps and Power Virtual Agents. By default, any user in the Azure AD Tenant can create additional environments. Enabling this control will restrict the creation of new environments to users with the following admin roles: Global admins, Dynamics 365 service admins, Power Platform Service admins, and Delegated admins.

2.1.1 Policy

- The ability to create additional environments SHALL be restricted to admins.

2.1.2 Resources

- Control who can create and manage environments in the Power Platform admin center | Microsoft Documents
- Environment Administrator | Digital Transformation Agency of Australia
- Microsoft Technical Documentation | Power Apps

2.1.3 License Requirements

- N/A

2.1.4 Implementation

1. Sign in to the Power Platform admin center or, for GCC environments, sign in to the GCC Power Platform Admin Center.
2. In the upper-right corner of the Microsoft Power Platform site, select the **Gear icon** (Settings icon).
3. Select **Power Platform settings**.
4. Under **Who can create production and sandbox environments**, select **Only specific admins.**
5. Under **Who can create trial environments**, select **Only specific admins.**

Now only Global admins, Dynamics 365 service admins, Power Platform Service admins, and Delegated admins can create environments.

2.2 Data Loss Prevention Policies for Power Platform Environments SHALL Be Created

To secure Power Platform environments, Data Loss Prevention (DLP) policies can be created to restrict the connectors that can be used with Power Apps created in an environment. A DLP policy can be created to affect all or some environments or exclude certain environments. The narrower policy will be enforced when there is a clash.

Connectors can be separated by creating a DLP policy that assigns them to one of three groups: Business, Non-Business, or Blocked. Connectors in different groups cannot be used in the same Power App. Connectors in the Blocked group cannot be used at all. Note that some M365 connectors cannot be blocked (e.g., Teams and SharePoint connectors).

In the DLP policy, connectors can also be configured to restrict read and write permissions to the data source/service. Connectors that cannot be blocked also cannot be configured. Agencies should evaluate the connectors and configure them to fit with agency needs and security requirements. The agency should then create a DLP policy to only allow those connectors to be used in the Power Platform.

When the Azure AD tenant is created, by default, a Power Platform environment is created in Power Platform. This Power Platform environment will bear the name of the tenant. There is no way to restrict users in the Azure AD tenant from creating Power Apps in the default Power Platform environment. Admins can restrict users from creating apps in all other created environments.

2.2.1 Policy

- A DLP policy SHALL be created to restrict connector access in the default Power Platform environment.
- Non-default environments SHOULD have at least one DLP policy that affects them.
- All connectors except those listed below SHOULD be added to the Blocked category in the default environment policy:
    - Approvals
    - Dynamics 365 Customer Voice
    - Excel Online (Business)
    - Microsoft Dataverse
    - Microsoft Dataverse (Legacy)
    - Microsoft Teams
    - Microsoft To-Do (Business)
    - Office 365 Groups
    - Office 365 Outlook
    - Office 365 Users
    - OneDrive for Business
    - OneNote (Business)
    - Planner
    - Power Apps Notification
    - Power BI
    - SharePoint
    - Shifts for Microsoft Teams
    - Yammer

2.2.2 Resources

- Data Policies for Power Automate and Power Apps | Digital Transformation Agency of Australia
- Create a data loss prevention (DLP) policy | Microsoft Docs

2.2.3 License Requirements

- N/A

2.2.4 Implementation

6. Sign in to the Power Platform admin center (for GCC environments sign in to the GCC Power Platform Admin Center).
7. On the left pane, select **Policies**, then **Data Policies.**
8. Select the **+ New Policy** icon to create a new policy.
9. Give the policy a suitable agency name and click **Next.**
10. In the **Prebuilt connectors** section, select the connectors that fit the agency's needs.
    a. Select a connector and click **Move to Business.**
    b. If necessary (and possible) for the connector, click **Configure connector** at the top of the screen to change connector permissions.
    c. Refer to Table 1 for those connectors to move which **Business/Non-Business** Category.
    d. For the default environment, move all connectors that cannot be blocked to the **Blocked** category.
    e. At the bottom of the screen, select **Next**.
11. Add a customer connector pattern that fit the agency's needs. Click **Next**.
12. Define the scope of the policy. For the default environment select **Add multiple environments** and add the default environment.
13. Select the environments over which to add the policy, and click **Add to policy** at the top.
14. Select **Next**-> **Create Policy** to finish.

2.3 Tenant Isolation SHALL Be Enabled to Prevent Cross Tenant Access of Power Platform environments

Power Platform tenant isolation is different from Azure AD-wide tenant restriction. It does not impact Azure AD-based access outside of Power Platform. Power Platform tenant isolation only works for connectors using Azure AD-based authentication, such as Office 365 Outlook or SharePoint. The default configuration in Power Platform is with tenant isolation set to **Off**, which allows for cross-tenant connections to be established. A user from tenant A using a Power App with a connector can seamlessly establish a connection to tenant B if using appropriate Azure AD credentials.

If admins want to allow only a select set of tenants to establish connections to or from their tenant, they can turn on tenant isolation. Once tenant isolation is turned on, inbound (connections to the tenant from external tenants) and outbound (connections from the tenant to external tenants) cross-tenant connections are blocked by Power Platform even if the user presents valid credentials to the Azure AD-secured data source.

2.3.1 Policy

- Power Platform tenant isolation SHALL be enabled.

- An inbound/outbound connection allowlist SHOULD be configured.
- The allowlist MAY be empty.

2.3.2 Resources

- Enable tenant isolation and configure allowlist | Microsoft Docs

2.3.3 License Requirements

- N/A

2.3.4 Implementation

1. Sign in to the Power Platform admin center or, for GCC environments, sign in to the GCC Power Platform Admin Center.
2. On the left pane, select **Policies -> Tenant Isolation**.
3. The tenant isolation allowlist can be configured by using **New tenant rule** on the Tenant Isolation page.
4. If Tenant Isolation is switched **Off**, add or edit the rules in the allowlist. However, these rules will not be enforced until tenant isolation is turned **On**.

2.4 Content Security Policy SHALL Be Enabled

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross-Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to malware distribution. Currently, there is no UI for editing these attributes, but there is a plan to expose this control in the Power Platform admin center. In the meantime, use this script to apply this setting. Also, there is no current way to implement this setting for Canvas Apps. When enabled, this setting will apply to all current Model-driven apps at only the environment level.

2.4.1 Policy

- Content security policies for model-driven Power Apps SHALL be enabled.

2.4.2 Resources

- Content Security Policy | Microsoft Docs

2.4.3 License Requirements

- N/A

2.4.4 Implementation

1. Sign in to Make Power Apps (for GCC environments sign in to the GCC Make Power Apps center).
2. On the left-hand pane select **Apps** and select one of the Model-Driven Apps (if there is no available Model-Driven app, create one).

3. While in the model-driven app menu with an account with entity update permissions, such as System Administrator or Power Platform Administrator, open the browser dev tools.
4. How to open the browser dev tools depends on which browser is used. For a chromium-based browser, right click -> **inspect** -> **console**.
5. Paste the JavaScript code found here into the console.
6. To enable CSP, pass the default configuration, i.e., call the function - enableFrameAncestors(["'self'"]).
7. As an example of enabling additional origins to embed the app - enableFrameAncestors(["*.powerapps.com", "'self'", "abcxyz"]).
8. To disable CSP call - disableCSP().

3 Acknowledgements

In addition to acknowledging the important contributions of a diverse team of Cybersecurity and Infrastructure Security Agency (CISA) experts, CISA thanks the following federal agencies and private sector organizations that provided input during the development of the Secure Business Cloud Application's security configuration baselines in response to Section 3 of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*:

- Consumer Financial Protection Bureau (CFPB)
- Department of the Interior (DOI)
- National Aeronautics and Space Administration (NASA)
- Sandia National Laboratories (Sandia)
- U.S. Census Bureau (USCB)
- U.S. Geological Survey (USGS)
- U.S. Office of Personnel Management (OPM)
- U.S. Small Business Administration (SBA)

The cross-agency collaboration and partnerships developed during this initiative serve as an example for solving complex problems faced by the federal government.

Cybersecurity Innovation Tiger Team (CITT) Leadership
Beau Houser (USCB), Sanjay Gupta (SBA), Michael Witt (NASA), James Saunders (OPM), Han Lin (Sandia), Andrew Havely (DOI).

CITT Authors
Trafenia Salzman (SBA), Benjamin McChesney (OPM), Robert Collier (USCB), Matthew Snitchler (Sandia), Darryl Purdy (USCB), Brandon Frankens (NASA), Brandon Goss (NASA), Nicole Bogeajis (DOI/USGS), Kevin Kelly (DOI), Adnan Ehsan (CFPB), Michael Griffin (CFPB), Vincent Urias (Sandia), Angela Calabaza (Sandia).

CITT Contributors

Dr. Mukesh Rohatgi (MITRE), Lee Szilagyi (MITRE), Nanda Katikaneni (MITRE), Ted Kolovos (MITRE), Thomas Comeau (MITRE), Karen Caraway (MITRE), Jackie Whieldon (MITRE), Jeanne Firey (MITRE), Kenneth Myers (General Services Administration).