Power Platform Governance and Administration

John Landgrave
Microsoft Corporation
Business Applications Platform Architect
Agenda

AN OVERVIEW OF MICROSOFT POWER PLATFORM ARCHITECTURE
SECURING YOUR ENVIRONMENTS
MONITORING AND MANAGING THE POWER PLATFORM

GETTING STARTED WITH THE POWER PLATFORM GOVERNANCE TOOLKIT
POWER PLATFORM DEVOPS AND DEPLOYMENT TECHNIQUES
BUILDING A CENTER OF EXCELLENCE
Agenda

- An Overview of Microsoft Power Platform Architecture
- Securing Your Environments
- Monitoring and Managing the Power Platform
- Getting Started with the Power Platform Governance Toolkit
- Power Platform DevOps and Deployment Techniques
- Building a Center of Excellence
Know your environments

Environments are containers that administrators can use to manage apps, flows, connections, and other assets; along with permissions to allow organization users to use the resources.
Know your environments

• Environments are tied to a geographic location that is configured at the time the environment is created.

• Environments can be used to target different audiences and/or for different purposes such as dev, test and production.

• Every tenant has a default environment, created automatically

• Common Data Service for Apps (CDS) databases are created in the context of environments; one per environment
PowerApps Environments are built on Azure

- PowerApps
- Logic Apps
- Functions
- Management API
- Storage
- Azure AD

PowerApps Default Environment
- PowerApps
- Flows
Office 365 Tenant and Default Environment

- Office 365 Tenant
- PowerApps Default Environment
  - PowerApps
  - Flows

- Azure AD
- Microsoft Azure
- Logic Apps
- Management API
- Functions
- Storage
Default Environment embedded connections

Office 365 Tenant
- SharePoint
- Teams
- Exchange
- Excel

PowerApps Default Environment
- PowerApps
- Flows

Microsoft Azure
- Azure AD
- Logic Apps
- Management API
- Functions
- Storage

- SharePoint
- Teams
- Exchange
- Excel
Environment Permissions in Default

Office 365 Tenant
- SharePoint
- Teams
- Exchange
- Excel

PowerApps Default Environment
- PowerApps
- Flows
- Makers: All Licensed Users: None

Azure AD
Microsoft Azure
- Logic Apps
- Functions
- Management API
- Storage
Using On Premise Data

Office 365 Tenant
- SharePoint
- Teams
- Exchange
- Excel

PowerApps Default Environment
- PowerApps
- Flows

Makers: All Licensed
Users: None

SharePoint
Exchange
Teams

Azure AD
Microsoft Azure

Data Gateway(s)
Logic Apps
Management API
Functions
Storage

On Premise Gateway(s)
Databases
Web API
SharePoint Data
File Storage

On Premise Systems
Provisioning New Environments

Office 365 Tenant
- Active Directory
- SharePoint
- Teams
- Exchange
- Excel

PowerApps
- Default Environment
  - PowerApps
  - Flows
  - Makers: All Licensed
  - Users: None

PowerApps Environment (no CDS)
- Canvas Apps
- Flows
- AD Managed
  - Makers: Admin
  - Users: None

PowerApps Environment (with CDS)
- Canvas Apps
- Flows
- Business Process Flows
- Managed by CDS (AD Groups)
  - Environment Admin: Creator
  - Environment Makers: None
  - System Customizer: None
  - CDS User: None

Azure AD
Microsoft Azure
- Logic Apps
- Management API
- Functions
- Storage

On Premise Gateway(s)
- Databases
- Web API
- SharePoint Data
- File Storage

On Premise Systems
Environment Data Loss Prevention
Prevent data leakage with DLP policies

- Data loss prevention policies (DLP) enforce rules for which connectors can be used together by classifying connectors as either Business Data only or No Business Data allowed.

- Simply, if you put a connector in the business data only group, it can only be used with other connectors from that group in the same app.

- Tenant admins can define policies that apply to all environments.
A Global Tenant Admin or Power Platform Service Admin can manage all environments.

An Environment Admin can manage any environment for which they have been granted Admin rights (creator has admin by default).

Currently (Entitlement Model) - any admin must also have a P2 license assigned for them to administer or create an environment.

Future (Capacity Model) – admins don’t need a P2 license to administer an environment, but they must have the admin privilege.
Environment Creation

Entitlement Model

• Must have a P2 license (including a Trial License)
• Can create up to 2 environments per P2 license

Capacity Model

• Any PowerApps licensed user can create an environment
• You can restrict this by using PowerShell to configure the DisableEnvironmentCreationByNonAdminUsers setting at the tenant level
• Only the Tenant Admin or members of the PowerPlatform Admin Group will be able to create new environments (if non-admins are disabled)
• Each environment requires 1GB of space before provisioning a new environment
PowerApps and Flow do not provide users with access to any data assets that they don’t already have access to. Users should only have access to data that they really require access to.

Network Access control policies can also apply to PowerApps and Flow. Blocking access to a site from within a network by blocking the sign-on page will also prevent connections to that site from being created in PowerApps & Flow.
PowerApps & Flow are Azure AD applications

Conditional Access

- Available for PowerApps and Microsoft Flow
- Azure AD Premium Required
- Scenario coverage:
  - Grant/Block access based upon:
    - User/Group
    - Device
    - Location

Microsoft Application Management (MAM) support
Monitoring and Management

**Proactive Management**

- Use Power Platform Admin Center to monitor activity
- Restrict user permissions in Premium environments
- Configure DLP Policies
- Use Active Directory to restrict access to data or systems

**Reactive Management**

- Monitor environments and remove assets or permissions based on policies
- Monitor audit records in Office Security and Compliance Center
- PowerShell cmdlets or Flows using management connectors
Power Platform Admin Center is the central management hub for all Power Platform activity (admin.powerplatform.microsoft.com).

Other Management interfaces will go away later this year (e.g. admin.powerapps.com, D365 Security Center).
DEMO

Power Platform Admin Center
How can I lock down <action X> to only <user Y> or lock down access to <data source Z>?

• How do I turn off individual plan sign-up (trials, Flow Free, community plans)?
• How do I restrict app creation in default env?
• How do I throttle environment creation?
• How do I control which makers are approved to use a connector?
• How do I control which apps are shared to a tenant?
• How do I control access to data in a service in scope for a user’s job but prevent access to data out of scope of their job?
• How do I enable an app to only read data through certain connectors and not write?
• How do I prevent use of a connector before it’s approved to be used?
• How do I control who can use a connector?
<table>
<thead>
<tr>
<th>PowerShell cmdlets for app creators (preview)</th>
<th>PowerShell cmdlets for administrator (preview)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read environments</td>
<td>Read, update, and delete environments &amp; Common Data Service databases Read, update, and delete environment permissions</td>
</tr>
<tr>
<td>Read, update, and delete a canvas app</td>
<td>Read, update, and remove canvas apps Read, update, and delete canvas app permissions</td>
</tr>
<tr>
<td>Read, update, and delete canvas app permissions</td>
<td>Read, update, and delete canvas app permissions</td>
</tr>
<tr>
<td>Read, update, and delete a flow</td>
<td>Read, update, and delete flows Read, update, and delete flow permissions</td>
</tr>
<tr>
<td>Read, update, and delete flow permissions</td>
<td>Read, update, and delete flow permissions</td>
</tr>
<tr>
<td>Read and respond to flow approvals</td>
<td></td>
</tr>
<tr>
<td>Read and delete connections</td>
<td>Read and delete connections Read, update, and delete connection permissions</td>
</tr>
<tr>
<td>Read, update, and delete connection permissions</td>
<td>Read, update, and delete connection permissions</td>
</tr>
<tr>
<td>Read and delete connectors</td>
<td>Read and delete custom connectors Read, update, and delete custom connector permissions</td>
</tr>
<tr>
<td>Read, update, and delete custom connector permissions</td>
<td></td>
</tr>
<tr>
<td>Read a user’s PowerApps user settings, user-app settings, and notifications Read &amp; delete a user’s Microsoft Flow settings</td>
<td></td>
</tr>
<tr>
<td>Read, update &amp; delete data loss prevention policies for your organization</td>
<td>Create, read, update &amp; delete data loss prevention policies for your organization</td>
</tr>
</tbody>
</table>
Build the policies you need with PowerApps, Microsoft Flow, and PowerShell

- Microsoft Flow Management Connector
- Flow Management Connector for Admins
- PowerApps Management Connector for Admins
- PowerApps Management Connector for App Makers
- Power platform for Admins

The new Management connectors provide the same level control but with added extensibility and ease-of-use by leveraging PowerApps and Flow.
## Control capabilities

<table>
<thead>
<tr>
<th>#</th>
<th>Capability</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>How do I restrict app/flow creation in default env?</td>
<td>Reactive – Flow <a href="aka.ms/restrictappcreators">aka.ms/restrictappcreators</a></td>
</tr>
<tr>
<td>2</td>
<td>How do I throttle environment creation?</td>
<td>Reactive – Flow <a href="aka.ms/restrictedenvcreators">aka.ms/restrictedenvcreators</a></td>
</tr>
<tr>
<td>3</td>
<td>How do I control which apps are shared to a tenant?</td>
<td>Reactive – Flow</td>
</tr>
<tr>
<td>4</td>
<td>How do I prevent use of a connector before it’s approved to be used?</td>
<td>Reactive – Flow <a href="aka.ms/newconnectornotification">aka.ms/newconnectornotification</a></td>
</tr>
<tr>
<td>5</td>
<td>How do I control who can use a connector?</td>
<td>Reactive – Flow <a href="aka.ms/restrictflowconnector">aka.ms/restrictflowconnector</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="aka.ms/restrictappconnector">aka.ms/restrictappconnector</a></td>
</tr>
<tr>
<td>6</td>
<td>How do I control access to data in a service in scope for a user’s job but prevent access to data out of scope of their job?</td>
<td>N/A – DLP only provide control at the connector-level But you can automate DLP policy creation <a href="aka.ms/dlppowershellscript">aka.ms/dlppowershellscript</a></td>
</tr>
<tr>
<td></td>
<td>E.g. Allow access to Enterprise storage in Box but prevent access to personal storage in Box.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>How do I enable an app to only read data through certain connectors and not write?</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>E.g. Read-only from Twitter and write to SharePoint.</td>
<td></td>
</tr>
</tbody>
</table>
DEMO

Remove App Permissions until Admin Approves App
Review the audit trail

- Activity Logging integrated with Office Security and Compliance center for comprehensive logging across Microsoft services like Dynamics 365 and Office 365.
- The audit records are stored in O365 Security and Compliance center.
- Office provides an API to query this data, which is currently used by many SIEM vendors to use the Activity Logging data for reporting.
Which activity logs are supported?

<table>
<thead>
<tr>
<th>Microsoft Flow</th>
<th>PowerApps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created flow</td>
<td>Created app</td>
</tr>
<tr>
<td>Edited flow</td>
<td>Edited/save app (draft)</td>
</tr>
<tr>
<td>Deleted flow</td>
<td>Published app</td>
</tr>
<tr>
<td>Edited permissions</td>
<td>Deleted app</td>
</tr>
<tr>
<td>Deleted permissions</td>
<td>Restored an app from app version</td>
</tr>
<tr>
<td>Started a paid trial</td>
<td>Launched app</td>
</tr>
<tr>
<td>Renewed a paid trial</td>
<td>Marking app as featured</td>
</tr>
<tr>
<td></td>
<td>Marking app as hero</td>
</tr>
<tr>
<td></td>
<td>Edited app permissions</td>
</tr>
<tr>
<td></td>
<td>Deleted app permissions</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Agenda

1. An Overview of Microsoft Power Platform Architecture
2. Securing Your Environments
3. Monitoring and Managing the Power Platform
4. Getting Started with the Power Platform Governance Toolkit
5. Power Platform DevOps and Deployment Techniques
6. Building a Center of Excellence
Power Platform Governance Toolkit

Open Source, Community Driven effort

PowerApps, Flows, PowerShell Scripts and PowerBI Dashboards

NO SUPPORT other than community-based support

https://aka.ms/GovernanceToolkit
Governance Toolkit Overview

SQL Server tables for:
- Environments
- Flows
- PowerApps
- PowerApps Connections

- Environment Inventory Flow
- PowerBI Dashboard
- Platform Manager PowerApp
Agenda

- An Overview of Microsoft Power Platform Architecture
- Securing Your Environments
- Monitoring and Managing the Power Platform
- Getting Started with the Power Platform Governance Toolkit
- Power Platform DevOps and Deployment Techniques
- Building a Center of Excellence
DevOps – Current State

Canvas Apps and Flows can be built and managed individually

- Export the PowerApp or Flow from one environment and import to another
- No automation for export or import
- Connections are recreated manually

Solutions

- Solutions are the DevOps packaging unit going forward
- Solution developers and testers need P1 or higher licenses
- Model Driven Application artifacts and CDS Entities are defined in solutions
- PowerShell script to tag existing Canvas apps and Flows as solution-aware
- Create all artifacts (including Canvas apps and Flows) from within a solution
DevOps – Future State

Solutions will have parameters soon

- Parameterized deployment of connections and flows
- Post Install processes

Power Platform Solutions will participate in Azure DevOps pipeline

“Treat environments like cattle, not pets”

- Create dev environment
- Check out existing solution
- Work on solution and check back in
- Delete dev environment
Agenda

AN OVERVIEW OF MICROSOFT POWER PLATFORM ARCHITECTURE
SECURING YOUR ENVIRONMENTS
MONITORING AND MANAGING THE POWER PLATFORM
GETTING STARTED WITH THE POWER PLATFORM GOVERNANCE TOOLKIT
POWER PLATFORM DEVOPS AND DEPLOYMENT TECHNIQUES
BUILDING A CENTER OF EXCELLENCE
Customer Adoption Maturity

- Briefings & Demos
- Proof of Concepts (PoCs)
- First Production App
- Multiple Production Apps
- Center of Excellence
Who is building solutions with the Power Platform?

**Professional IT developers**
- Enables high productivity app development
- Reduces time to develop and deploy
- Centrally managed and rolled out

**Citizen developers**
- Lower barrier of entry for app development
- Power users in business units close to the problem building solutions for their teams
- Often with IT oversight or in an approved sandbox
Responsibilities of a Center of Excellence

1. Administration and governance
2. Evangelism and training
3. App development & technical support
4. Data + API Strategy
5. ALM + Infrastructure automation
6. Tools + Best practices
7. End user Support
Questions?