




# Automate Microsoft Defender for Cloud Alerts using Logic Apps

This project demonstrates how to automate security recommendations from Microsoft Defender for Cloud using Logic Apps (Standard), the modern approach to security orchestration in Azure.

Modern Portal Walkthrough – 2025 Edition (Workflow Standard Plan)

 #PerparimLabs | Azure Security Automation



# Objective


**Goal:** Set up a Logic App to automatically send email notifications when new **Defender for Cloud recommendations** are triggered — demonstrating automation in modern Azure environments.

Logic Apps enable security teams to respond automatically when new risks are detected, reducing mean time to respond (MTTR) and ensuring consistent alert handling.

# Create Logic App (Workflow Standard Plan)

- Created a new Logic App using the **Workflow Standard** plan, with integrated storage and Application Insights monitoring enabled.

The Standard plan hosts the Logic App on an App Service Plan for enterprise scalability and hybrid connectivity. It replaces the legacy Consumption model.

 **Note:** The new portal defaults to the **Standard hosting plan**, replacing the older Consumption model.

[All services](#) > [Logic apps](#) > [Create Logic App](#) >

## Create Logic App (Workflow Service Plan) ...

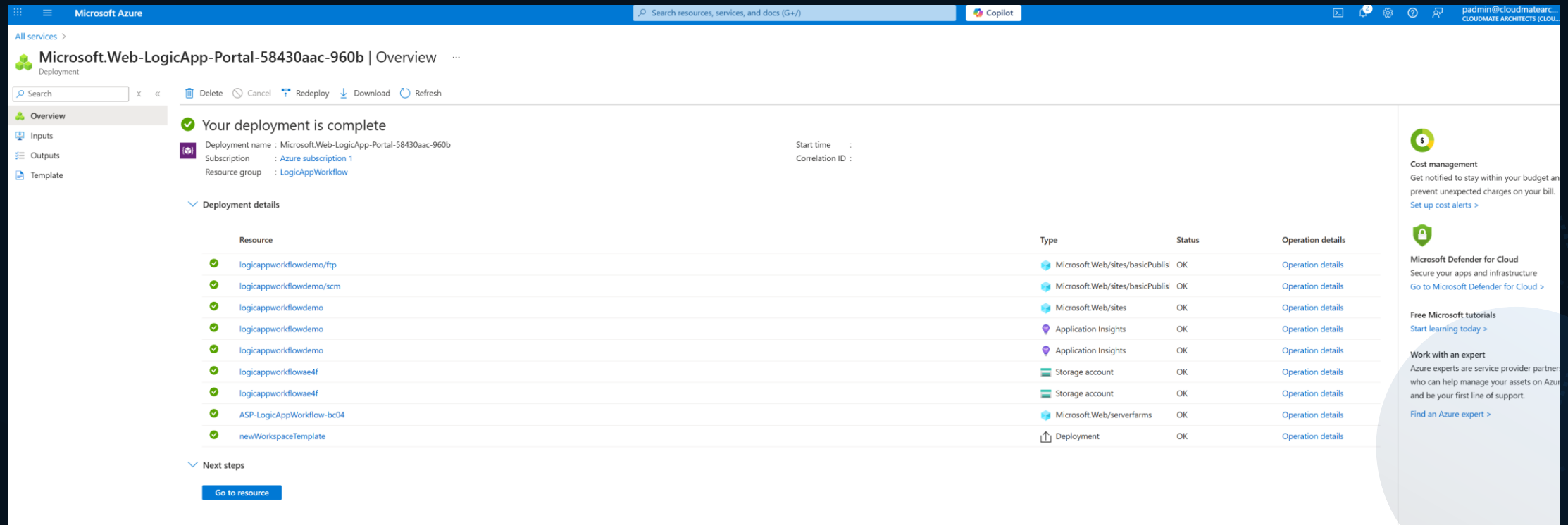
<b>Details</b>	
Subscription	
Resource Group	LogicAppWorkflow
Name	logicappworkflowdemo
<b>Hosting</b>	
<b>Storage (New)</b>	
Storage account	logicappworkflowae4f
<b>Plan (New)</b>	
Hosting options and plans	Workflow Standard
Name	ASP-LogicAppWorkflow-bc04
Operating System	Windows
Region	Canada Central
SKU	Workflow Standard
Size	Small
ACU	210 total ACU
Memory	3.5 GB memory
<b>Monitoring (New)</b>	
Application Insights	Enabled
Name	logicappworkflowdemo
Region	Canada Central
<b>Deployment</b>	
Basic authentication	Disabled
Continuous deployment	Not enabled / Set up after app creation
<b>Authentication</b>	
<b>Host storage (AzureWebJobsStorage)</b>	
Name	logicappworkflowae4f
Role	Not applicable when using secrets
<b>Azure Files</b>	
Name	logicappworkflowae4f
Role	Not applicable when using secrets
<b>Application Insights</b>	
Name	logicappworkflowdemo
Role	Not applicable when using secrets

[Create](#) [Previous](#) [Next >](#) [Download a template for automation](#)

# Deployment Complete

- Deployment succeeded — confirming Logic App, Storage Account, and App Service Plan resources created successfully.

App Service, Storage Account, and Application Insights are provisioned automatically to provide persistence, logging, and monitoring for each workflow run.



**Microsoft Azure** | Search resources, services, and docs (G+/) | Copilot | padmin@cloudmatearc... CLOUDMATE ARCHITECTS (CLOU...

All services > **Microsoft.Web-LogicApp-Portal-58430aac-960b** | Overview

Deployment

Search x < Delete Cancel Redeploy Download Refresh

**Overview**

Inputs

Outputs

Template

**Your deployment is complete**

Deployment name : Microsoft.Web-LogicApp-Portal-58430aac-960b

Subscription : Azure subscription 1

Resource group : LogicAppWorkflow

Start time :

Correlation ID :

**Deployment details**

Resource	Type	Status	Operation details
logicappworkflowdemo/ftp	Microsoft.Web/sites/basicPublicis	OK	<a href="#">Operation details</a>
logicappworkflowdemo/scm	Microsoft.Web/sites/basicPublicis	OK	<a href="#">Operation details</a>
logicappworkflowdemo	Microsoft.Web/sites	OK	<a href="#">Operation details</a>
logicappworkflowdemo	Application Insights	OK	<a href="#">Operation details</a>
logicappworkflowdemo	Application Insights	OK	<a href="#">Operation details</a>
logicappworkflowae4f	Storage account	OK	<a href="#">Operation details</a>
logicappworkflowae4f	Storage account	OK	<a href="#">Operation details</a>
ASP-LogicAppWorkflow-bc04	Microsoft.Web/serverfarms	OK	<a href="#">Operation details</a>
newWorkspaceTemplate	Deployment	OK	<a href="#">Operation details</a>

**Next steps**

[Go to resource](#)

**Cost management**

Get notified to stay within your budget and prevent unexpected charges on your bill.

[Set up cost alerts >](#)

**Microsoft Defender for Cloud**

Secure your apps and infrastructure

[Go to Microsoft Defender for Cloud >](#)

**Free Microsoft tutorials**

[Start learning today >](#)

**Work with an expert**

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

[Find an Azure expert >](#)

# Create Workflow

- Inside the Logic App, added a new workflow named **defenderworkflow** using the **Stateful** mode — optimized for long-running, reliable processes.

The screenshot shows the 'Create workflow' dialog in the Microsoft Azure portal. The 'Workflow name' is 'defenderworkflow'. The 'Stateful' mode is selected, indicated by a blue circle. The dialog includes a table comparing workflow types:

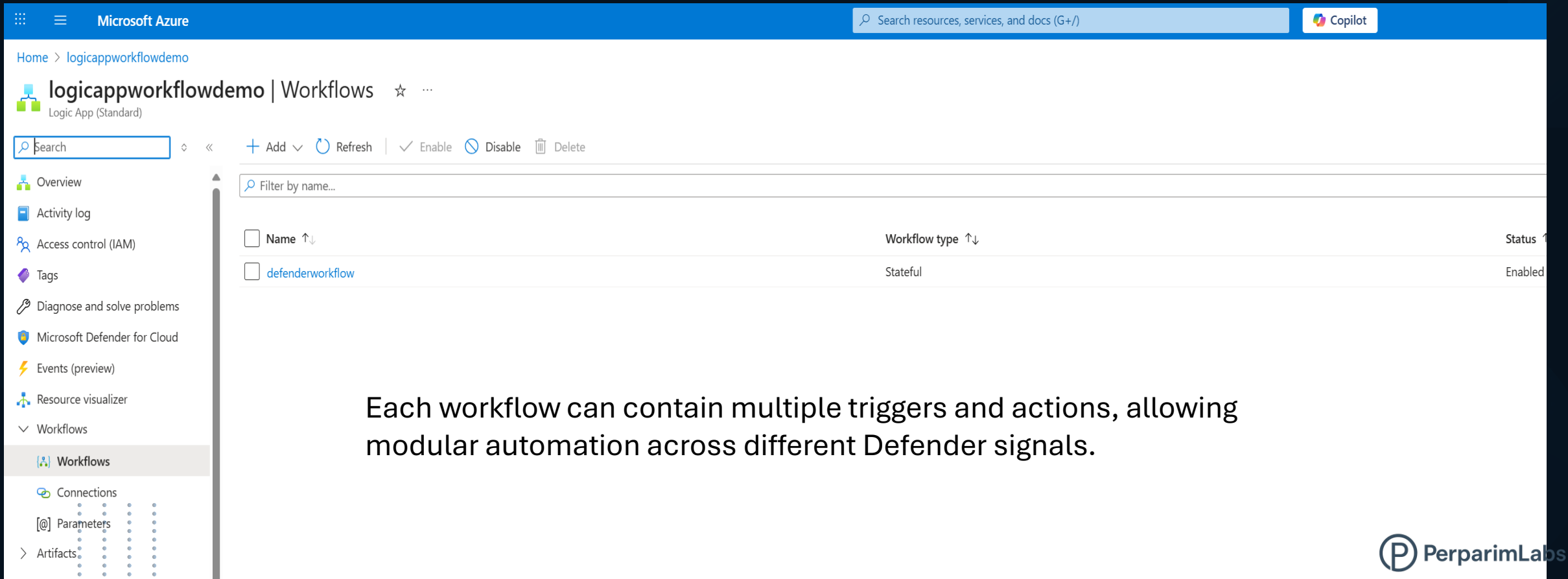
	Autonomous Agents (Preview)	Conversational Agents (Preview)	Stateful	Stateless
	Stateful workflows use AI agents to complete tasks and can start from any trigger, such as an event, schedule, or API call.	Stateful workflows use AI agents to complete tasks through chat interactions or other agents.	Optimized for high reliability, ideal for process business transitional data.	Optimized for low latency, ideal for request-response and processing IoT events.
Support for agents	✓	✓	✓	--
Support Agent-to-Agent (A2A) protocol	--	✓	--	--
Multi-agent patterns	✓	✓	✓	--
Any available trigger	✓	--	✓	✓
Run fast	--	--	--	✓
Store workflow run history	✓	✓	✓	--
Run asynchronously	✓	✓	✓	--
Support long-running workflows	✓	✓	✓	--
Handle large data	✓	✓	✓	--

The 'Create' button is highlighted in blue.

A “Stateful” workflow stores run-history and output, critical for auditing and post-incident analysis in SOC environments.

# Workflow Created

- Workflow successfully created and enabled — ready to define triggers and actions.



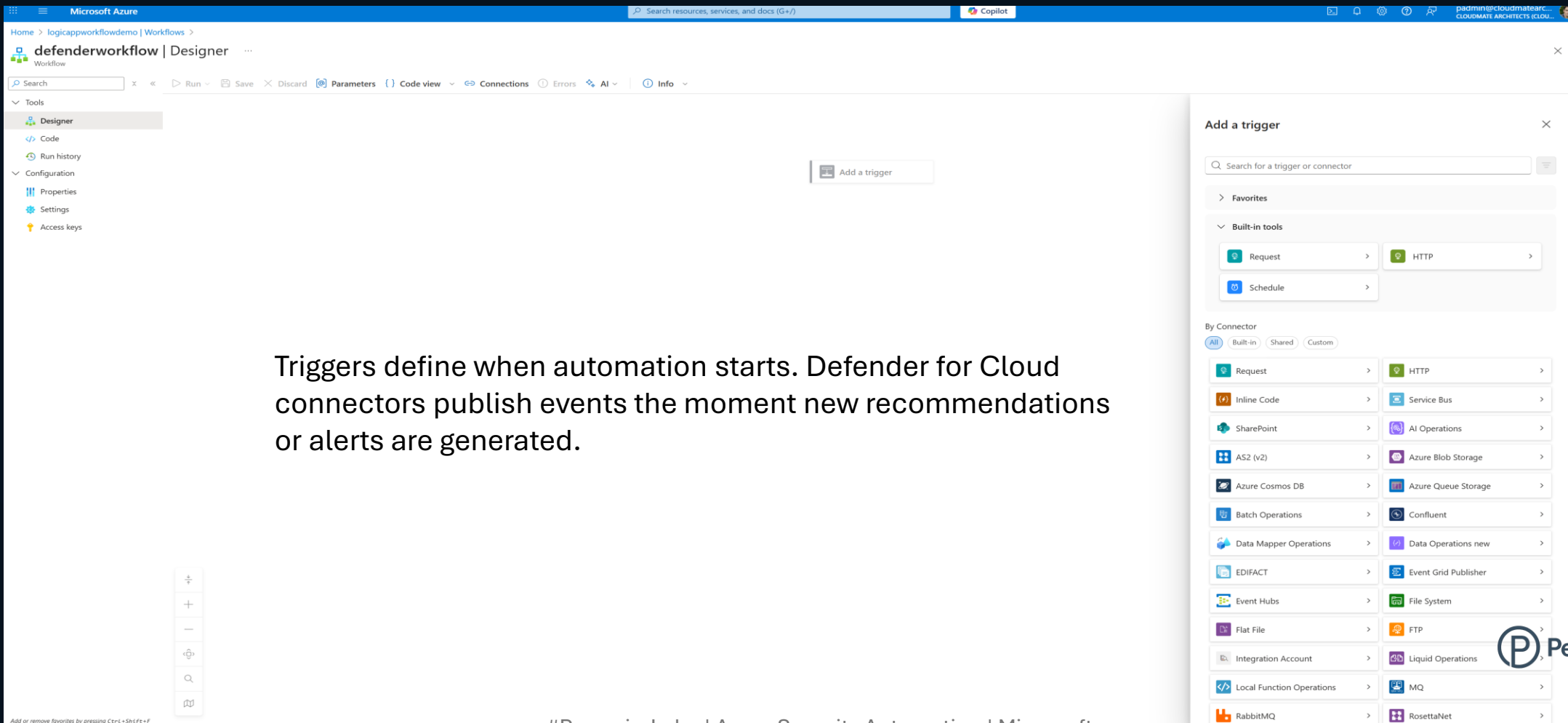
The screenshot displays the Microsoft Azure portal interface. At the top, the 'Microsoft Azure' header includes a search bar and the 'Copilot' button. The breadcrumb trail shows 'Home > logicappworkflowdemo'. The main heading is 'logicappworkflowdemo | Workflows', with a star icon and a dropdown menu. Below this, a search bar and action buttons ('Add', 'Refresh', 'Enable', 'Disable', 'Delete') are visible. A left-hand navigation pane lists various options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Microsoft Defender for Cloud, Events (preview), Resource visualizer, Workflows (selected), Connections, Parameters, and Artifacts. The main content area features a 'Filter by name...' search bar and a table of workflows. The table has columns for 'Name', 'Workflow type', and 'Status'. One workflow is listed: 'defenderworkflow' with a 'Stateful' type and 'Enabled' status.

Name ↑↓	Workflow type ↑↓	Status
defenderworkflow	Stateful	Enabled

Each workflow can contain multiple triggers and actions, allowing modular automation across different Defender signals.

# Add Trigger

- Opened the **Designer** and selected the trigger source. Logic Apps Designer now provides built-in connectors for Defender, Azure, and third-party integrations.



Triggers define when automation starts. Defender for Cloud connectors publish events the moment new recommendations or alerts are generated.

# Defender Trigger

- Selected **“When a Microsoft Defender for Cloud recommendation is created or triggered.”**  
This ensures automation activates instantly when new security recommendations are generated.

The screenshot shows the Microsoft Azure Logic App Designer interface. The main canvas is empty, and the 'Add a trigger' panel is open on the right. The panel lists several triggers under the 'Microsoft Defender for Cloud' category. The trigger 'When a Microsoft Defender for Cloud Recommendation is created or triggered' is selected. The left sidebar shows the 'Tools' section with 'Designer' selected. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'padmin@cloudmatearc... CLOUDMATE ARCHITECTS (CLOUD...)'. The bottom right corner features the PerparimLabs logo.

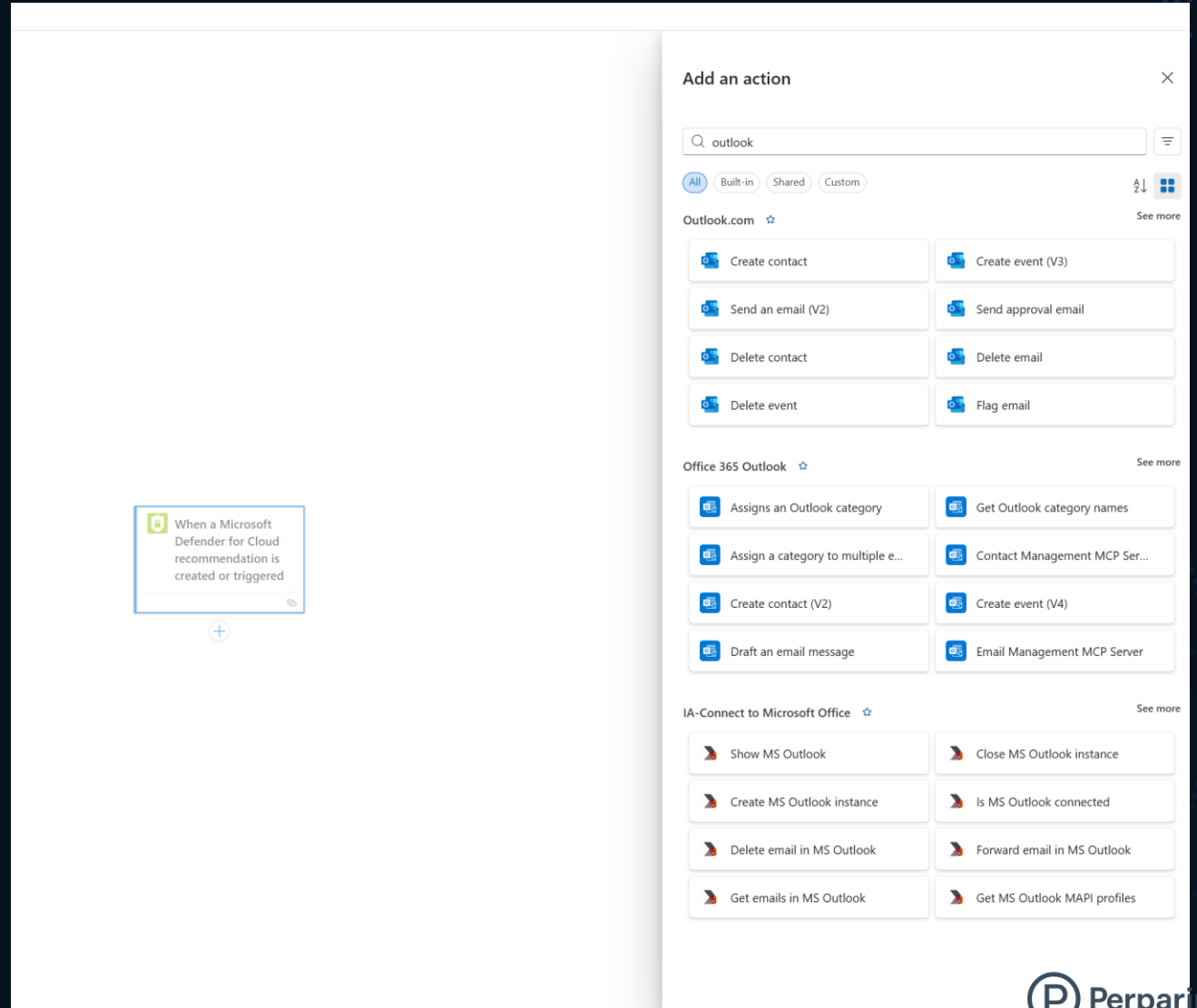
Selecting this trigger binds the workflow directly to Defender’s recommendation API—no need for manual polling or scripts.



# Add Email Action

- Added an **Outlook (V2) Send Email** action to automatically alert the admin mailbox.

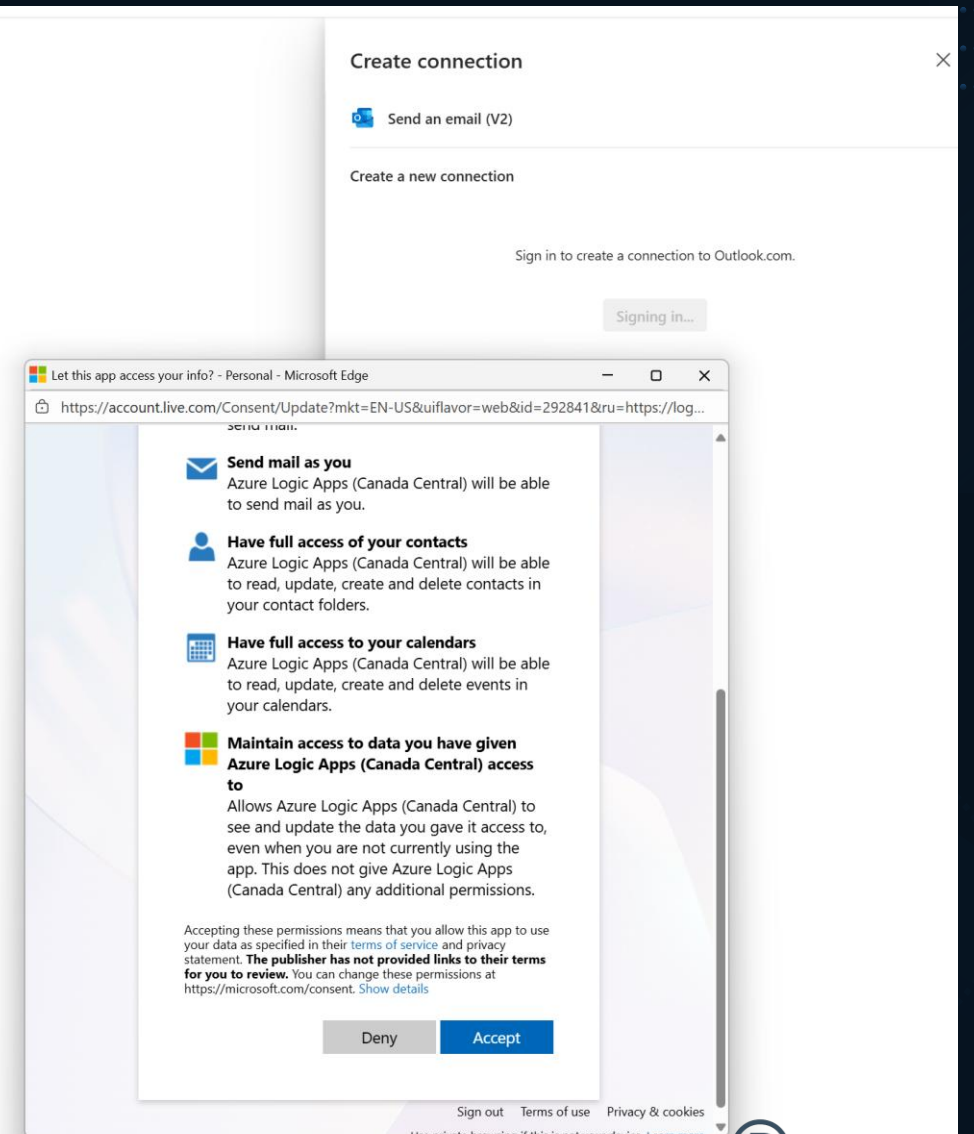
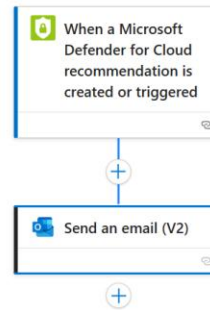
The Outlook connector is a quick notification channel; in production, this could integrate with Teams, ITSM, or Sentinel Playbooks.



# Connect Outlook

- Authorized Azure Logic Apps (Canada Central) to send email using the connected Outlook account.

Uses secure OAuth 2.0 delegated permissions—no stored credentials—ensuring compliance with least-privilege principles.



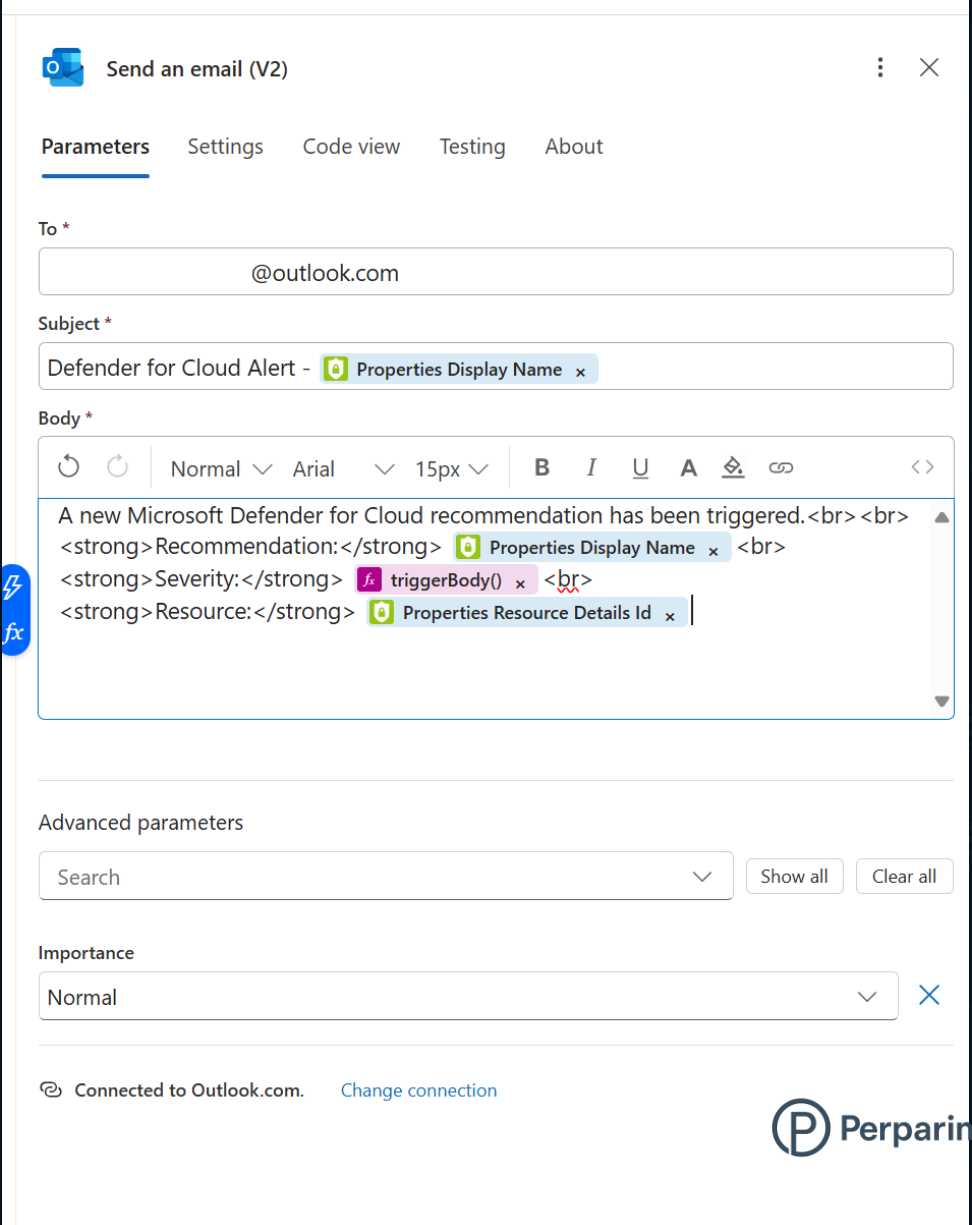
# Configure Email Content

- Customized the email body with dynamic content:

- **Recommendation name**
- **Severity**
- **Resource details**

Dynamic content tokens pull real-time data (recommendation name, severity, resource ID) directly from Defender payloads, making alerts actionable.

 **Tip:** You can format the body with HTML for rich, readable alerts.



**Send an email (V2)**

Parameters Settings Code view Testing About

To \*  
@outlook.com

Subject \*  
Defender for Cloud Alert - Properties Display Name x

Body \*  
A new Microsoft Defender for Cloud recommendation has been triggered.<br><br><strong>Recommendation:</strong> Properties Display Name x <br><strong>Severity:</strong> triggerBody() x <br><strong>Resource:</strong> Properties Resource Details Id x


Advanced parameters  
Search Show all Clear all

Importance  
Normal x

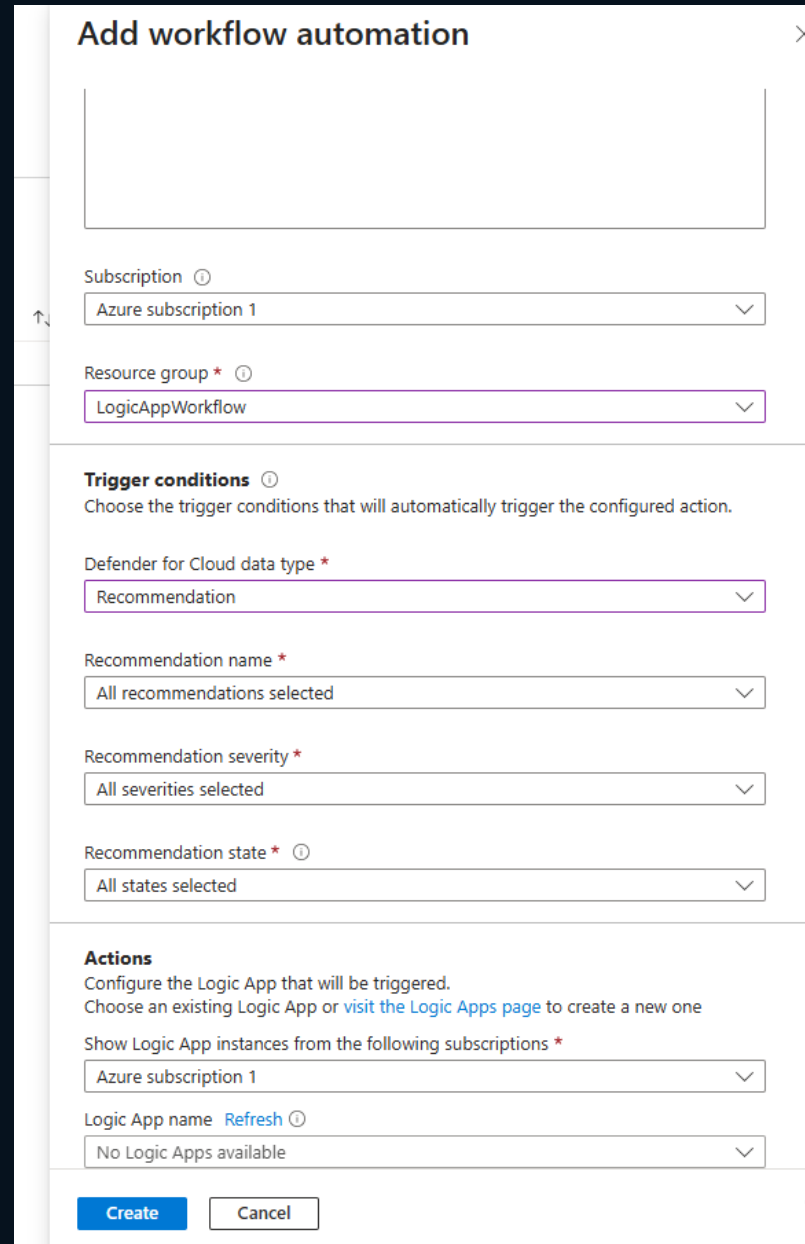
Connected to Outlook.com. Change connection

PerparimLabs

# Defender Workflow Automation Setup

- Opened **Defender for Cloud** → **Workflow Automation** to connect the Logic App. However, modern environments currently show:
- “No Logic Apps available”
-  *Reason:* Logic App (Standard) resources are not yet discoverable from Defender for Cloud automation panel — only **Consumption plans** appear there.

As of 2025, Defender for Cloud’s automation pane lists only Consumption Logic Apps. Standard-plan Logic Apps integrate through native triggers instead.



**Add workflow automation**

Subscription ⓘ  
Azure subscription 1

Resource group \* ⓘ  
LogicAppWorkflow

**Trigger conditions** ⓘ  
Choose the trigger conditions that will automatically trigger the configured action.

Defender for Cloud data type \*  
Recommendation

Recommendation name \*  
All recommendations selected

Recommendation severity \*  
All severities selected

Recommendation state \* ⓘ  
All states selected

**Actions**  
Configure the Logic App that will be triggered.  
Choose an existing Logic App or [visit the Logic Apps page](#) to create a new one

Show Logic App instances from the following subscriptions \*  
Azure subscription 1

Logic App name [Refresh](#) ⓘ  
No Logic Apps available

**Create** **Cancel**

# Summary

## ✓ Lab Completed:


- Built Logic App with Defender trigger and Outlook alert.
- Observed modern portal limitations (Standard vs. Consumption).
- Demonstrated full automation workflow concept.


This architecture establishes a reusable pattern: detect → notify → remediate.  
Future enhancements can add playbooks, ticket creation, or auto-remediation.

## 🧠 Key Takeaway:

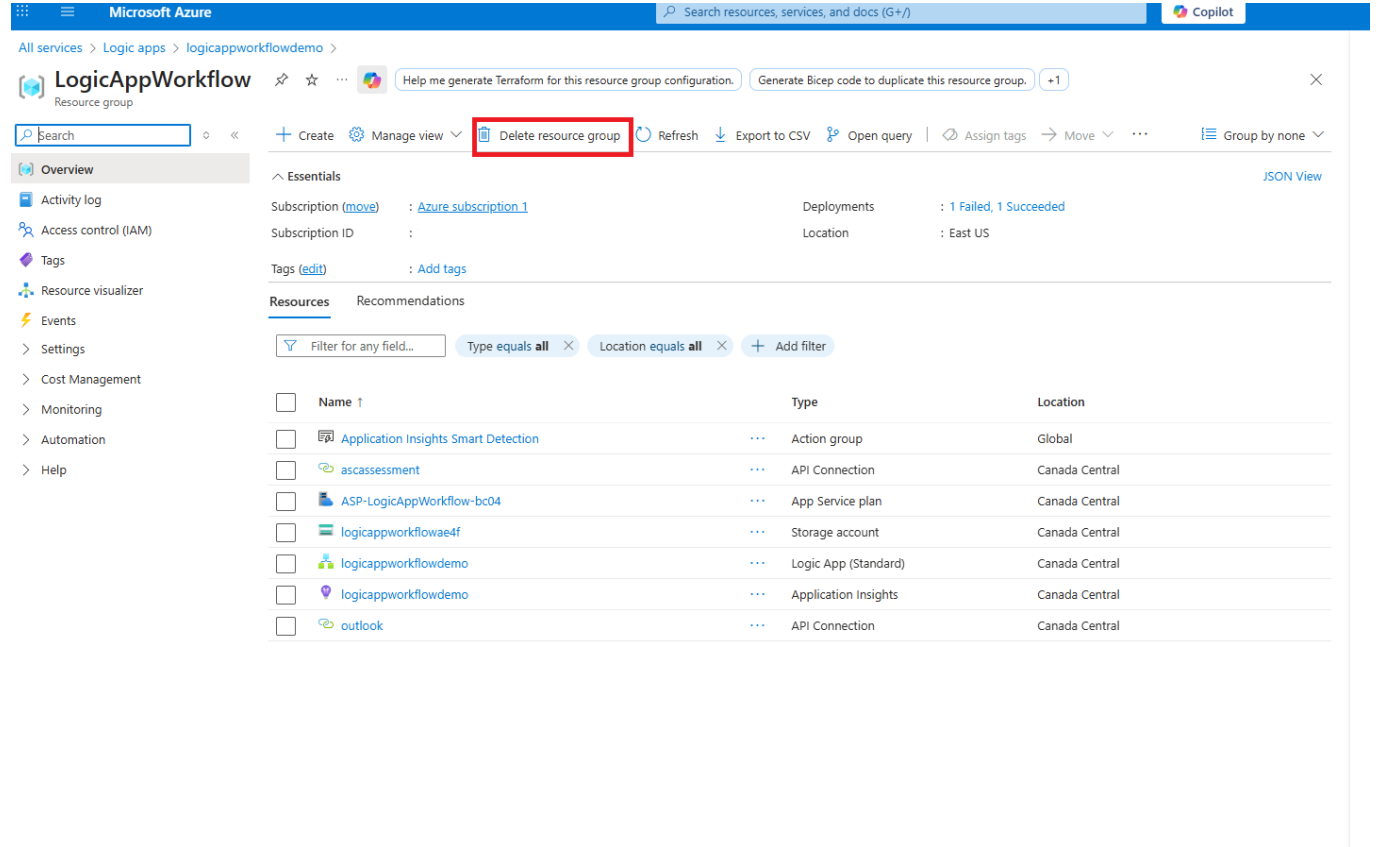
Microsoft Defender for Cloud automation now integrates with **Logic Apps Standard**, but configuration visibility in Defender UI will be updated in future releases.

# Cleanup

 Delete the resource group **LogicAppWorkflow** to stop charges.

 Always remove unused Standard Logic Apps — they run under App Service Plans and can accumulate small costs.

Standard Logic Apps run persistently—deleting the resource group immediately halts compute billing.



The screenshot shows the Microsoft Azure portal interface for the 'LogicAppWorkflow' resource group. The 'Delete resource group' button is highlighted with a red box. The 'Resources' section lists various resources including Application Insights, API Connections, App Service Plan, Storage account, Logic App, and Application Insights.

Name	Type	Location
Application Insights Smart Detection	Action group	Global
ascassessment	API Connection	Canada Central
ASP-LogicAppWorkflow-bc04	App Service plan	Canada Central
logicappworkflowae4f	Storage account	Canada Central
logicappworkflowdemo	Logic App (Standard)	Canada Central
logicappworkflowdemo	Application Insights	Canada Central
outlook	API Connection	Canada Central