SharePoint Online and OneDrive for Business Enablement

Installation Guide v1.3

Tryg

Document Information

|  |  |
| --- | --- |
| Authors | Brian Jacobsen |
| Status | Final |

History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Modified by | Changes |
| 0.1 | 2018-03-05 | Brian Jacobsen | Initial Version – R1 deployment |
| 0.2 | 2018-03-08 | Mikael Nilsson | Reviewed |
| 0.3 | 2018-03-09 | John Garner | Reviewed |
| 1.0 | 2018-03-09 | Mikael Nilsson | Baselined |
| 1.1 | 2018-03-13 | Brian Jacobsen | Domain whitelisting |
| 1.2 | 2018-03-13 | Rolands Strakis | Flow import configurations |
| 1.3 | 2018-03-17 | Mikael Nilsson | Notes from deployment |
|  |  |  |  |

Contents

[1 Overview 4](#_Toc509238714)

[1.1 Abbreviations 4](#_Toc509238715)

[2 Tenant configurations 5](#_Toc509238716)

[2.1 DLP policies 5](#_Toc509238717)

[2.2 Office 365 Labels with retention 5](#_Toc509238718)

[2.3 Office 365 Group Expiration 6](#_Toc509238719)

[2.4 White listing 7](#_Toc509238720)

[2.5 Configure-O365Groups.ps1 script 7](#_Toc509238721)

[2.5.1 Site classification labels 8](#_Toc509238722)

[2.5.2 Office 365 Group naming convention 8](#_Toc509238723)

[2.6 MS Flow data policies 8](#_Toc509238724)

[2.7 SPO AppId + AppSecret creation 8](#_Toc509238725)

[3 Deploy Custom Services and Azure Resources 12](#_Toc509238726)

[3.1 Deploy the REST Service 12](#_Toc509238727)

[3.2 Deploy Azure Function 13](#_Toc509238728)

[3.3 Deploy MS Flow Workflow 18](#_Toc509238729)

[3.4 Deploy SharePoint Site Script, Site Design and Theme 19](#_Toc509238730)

# Overview

This document describes the tasks required to deploy and configure the solution, note that actual configuration values are tracked in the CIL documentation.

## Abbreviations

|  |  |
| --- | --- |
| Resource name | Description |
| CIL | Configuration Item List - SPO Platform CIL ver. x.x.xlsx |
| O365 | Office 365 |
| SPO | SharePoint Online |
| AAD | Azure Active Directory |
| DLP | Data Loss Prevention |
| CSOM | Client Site Object Model |
|  |  |
|  |  |

# Tenant configurations

## DLP policies

For policy configuration, please follow steps form “SPO and OD4B Enablement Design v1.0.docx” section 3.6.4.

## Office 365 Labels with retention

The site classification labels are created in the Office 365 Security & Compliance center

3 labels are created:

* Personal
* Internal
* Confidential

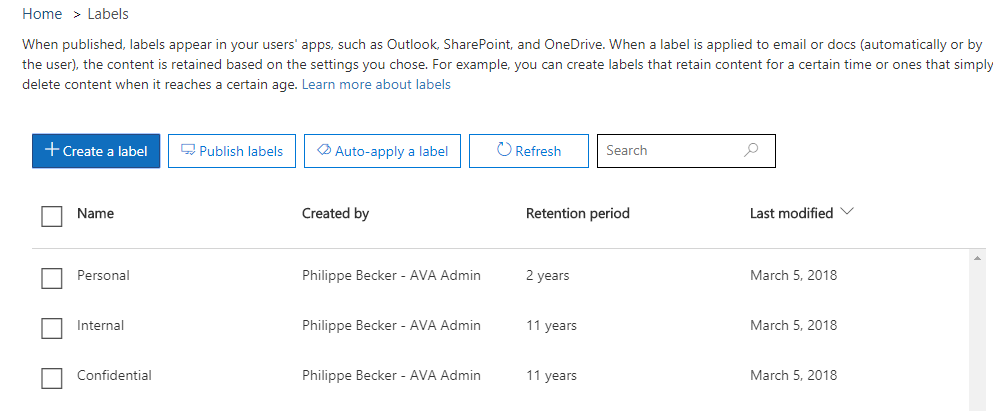
These labels must correspond with the Office 365 Group Site Classifications

The configuration for the labels is outlined in the CIL documentation.

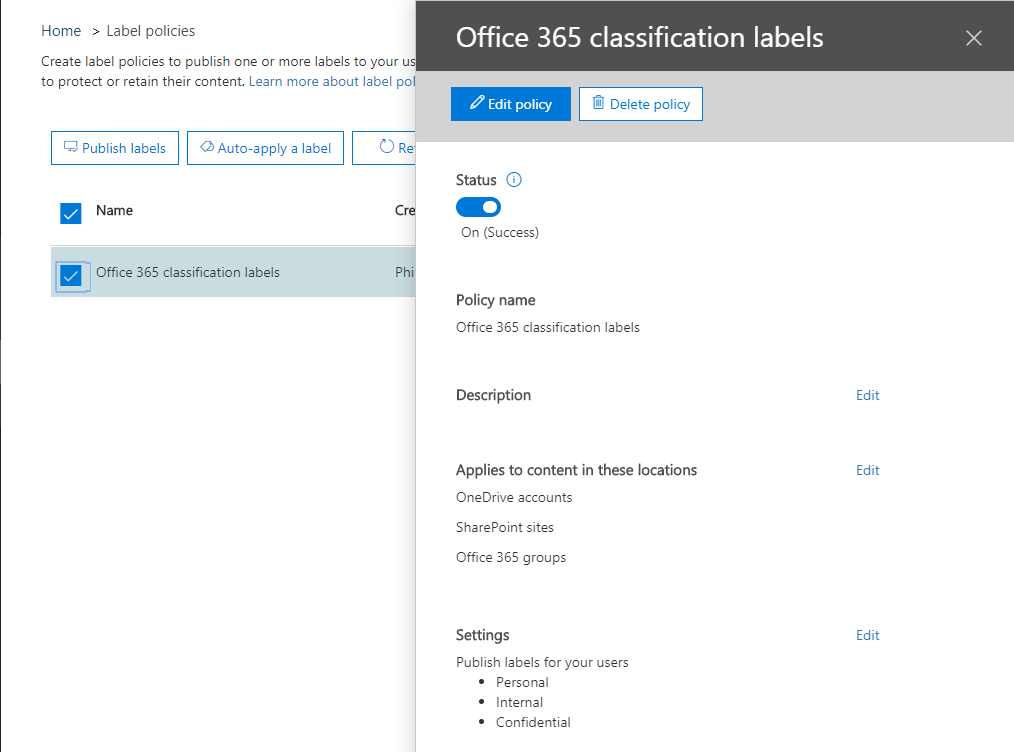
These labels must be published.

Steps:

* Open the Office 365 admin portal as a global administrator
* Select the Security & Compliance center
* Select Classifications -> Labels
* Select “Create a label”
* Configure labels as per CIL



* Select Label Policies
* Select Publish labels
* Publish all 3 labels as per CIL

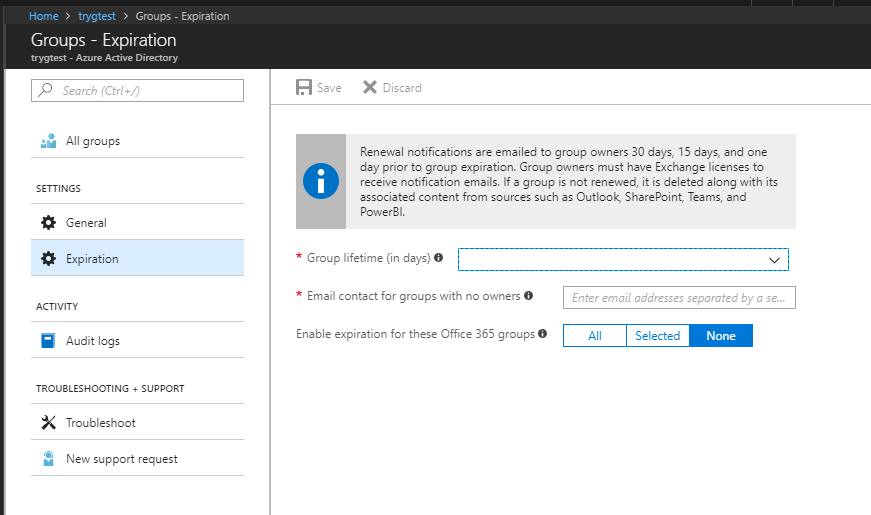


* The site classifications can take 15-60 minutes before they are available

## Office 365 Group Expiration

The Office 365 Group Expiration is configured in the AAD admin center

* Open the Azure Admin Center https://portal.azure.com with a global admin
* Select the “Azure Active Directory” admin center
* Select “Azure Active Directory”
* Select “Groups”
* Select “Expiration”
* Configure the group expiration time as per CIL

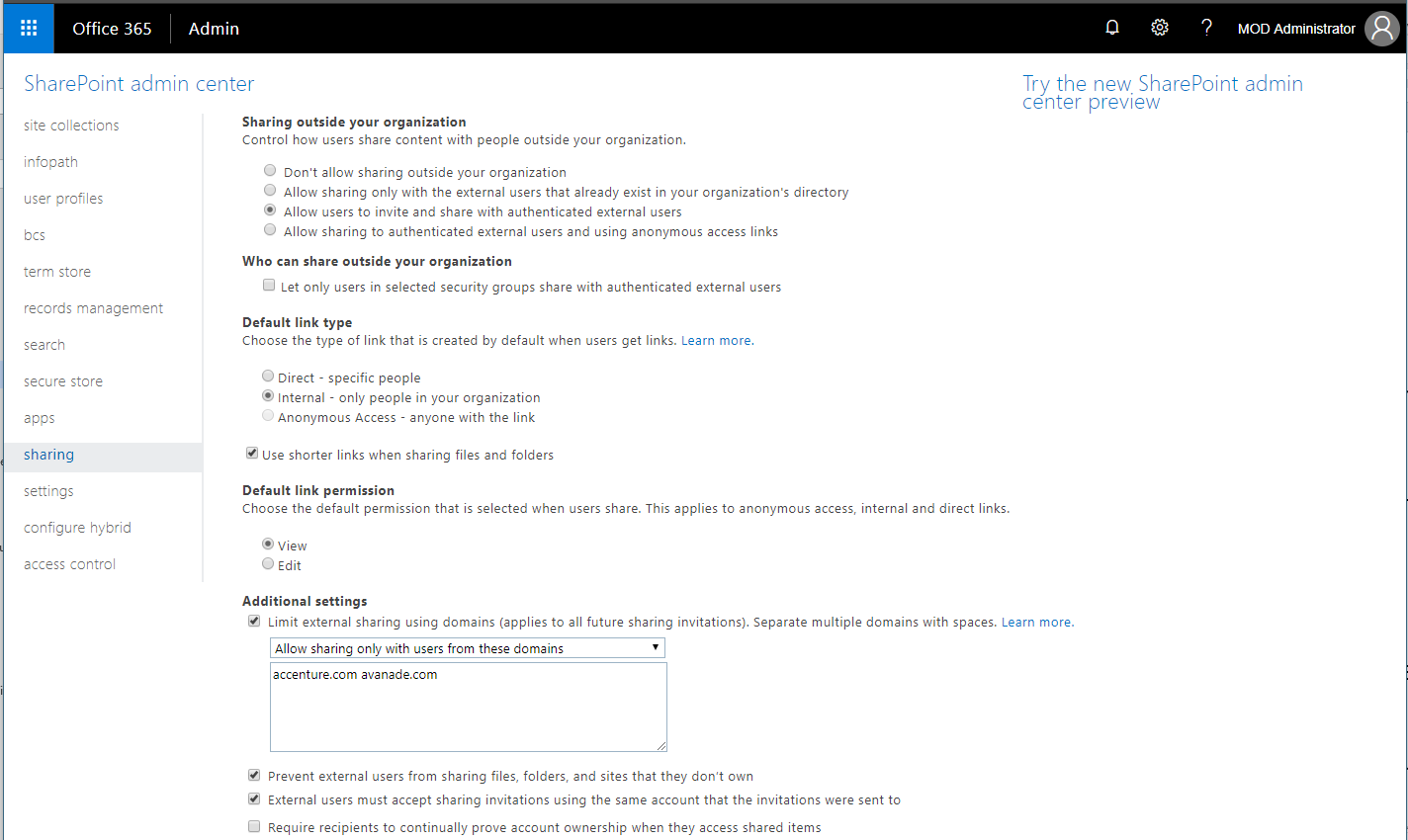


## White listing

The white listing of domains is configured in both SharePoint Online and in Azure AD.

SharePoint Online white listing through the SharePoint Online admin center, “sharing” option

* Select the “Limit external sharing using domains”
* Update the list as per the CIL (divide multiple with spaces)



Azure AD (Office 365 Groups) white listing is updated through the AzureADPreview PowerShell module and a Microsoft provided PowerShell script:

* Documentation - <https://technet.microsoft.com/en-us/library/mt842200(v=exchg.150).aspx>
* Download - <https://www.microsoft.com/en-us/download/details.aspx?id=55709>

The commands required are:

* Unless installed:
  + Install-Module AzureADPreview
* Connect-AzureAD
* Set-GuestAllowBlockDomainPolicy.ps1 -Update -AllowList @("avanade.com", "accenture.com")
  + NOTE! This will overwrite whatever domains we have in there. For future additions use:  
    Set-GuestAllowBlockDomainPolicy.ps1 -Append -AllowList @("contoso.com")

It will take some time before the tenant is fully configured.

## Configure-O365Groups.ps1 script

This script must be executed to configure some of the basic elements of Office 365 Group

* Open a PowerShell prompt as a Windows administrator
* If the “AzureADPreview” module isn’t installed, then execute
  + Install-Module AzureADPreview
* If the “AzureADPreview” module is installed, then execute
  + Update-Module AzureADPreview
* Execute the script

The configuration elements performed are outlined in the below subchapters.

### Site classification labels

The site classification labels are created through the execution of the “Configure-O365Groups.ps1” script

These must correspond with the labels added in the Security & Compliance center.

This script will also set the “Usage guidelines” link visible on the Create Site form.

### Office 365 Group naming convention

The Office 365 groups naming standard is configured through the execution of the “Configure-O365Groups.ps1” script

The naming standard will only apply to non-admins.

The CIL will contain the actual naming standard applied.

## MS Flow data policies

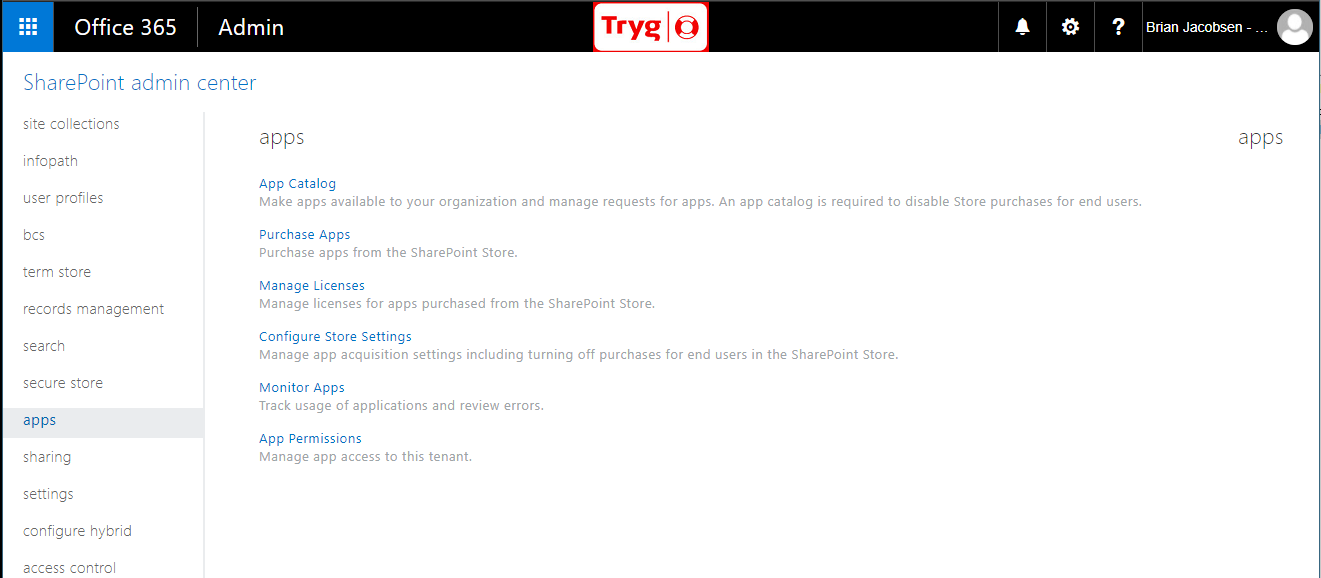
The data loss prevention policies

* Open https://admin.flow.microsoft.com with a global admin
* Select “Data Policies”
* Select “New Policy” for “All Environments”
* Configure the DLP policy as per the CIL

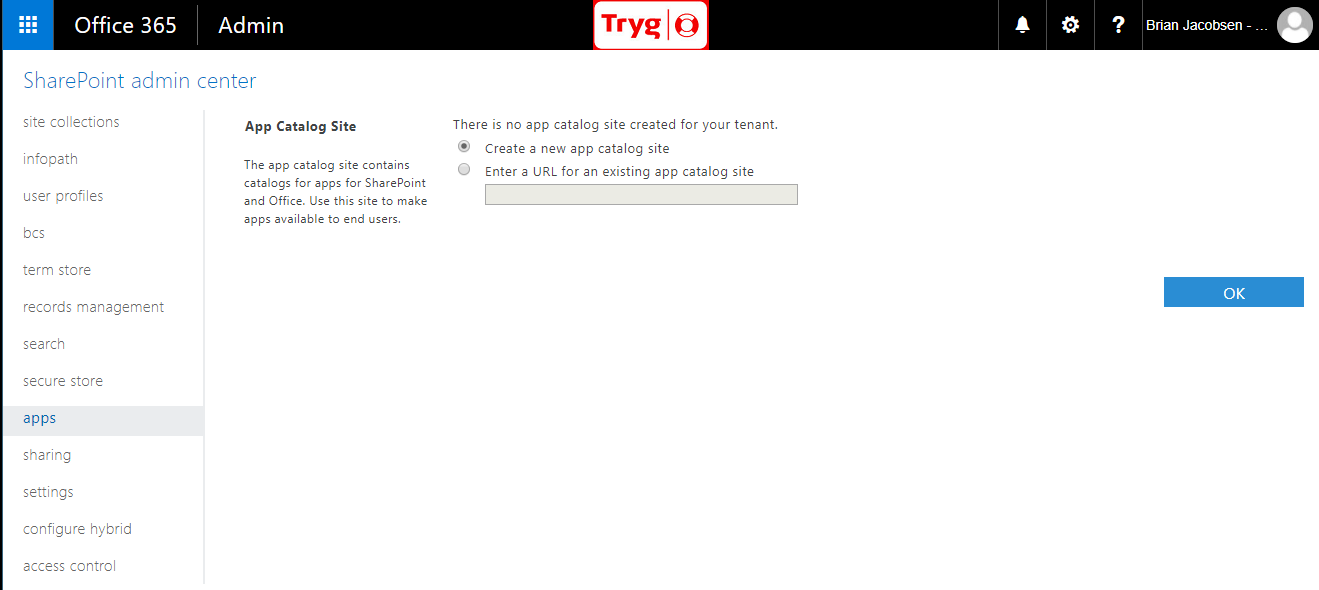
## SPO AppId + AppSecret creation

The process to create the AppId/AppSecret is:

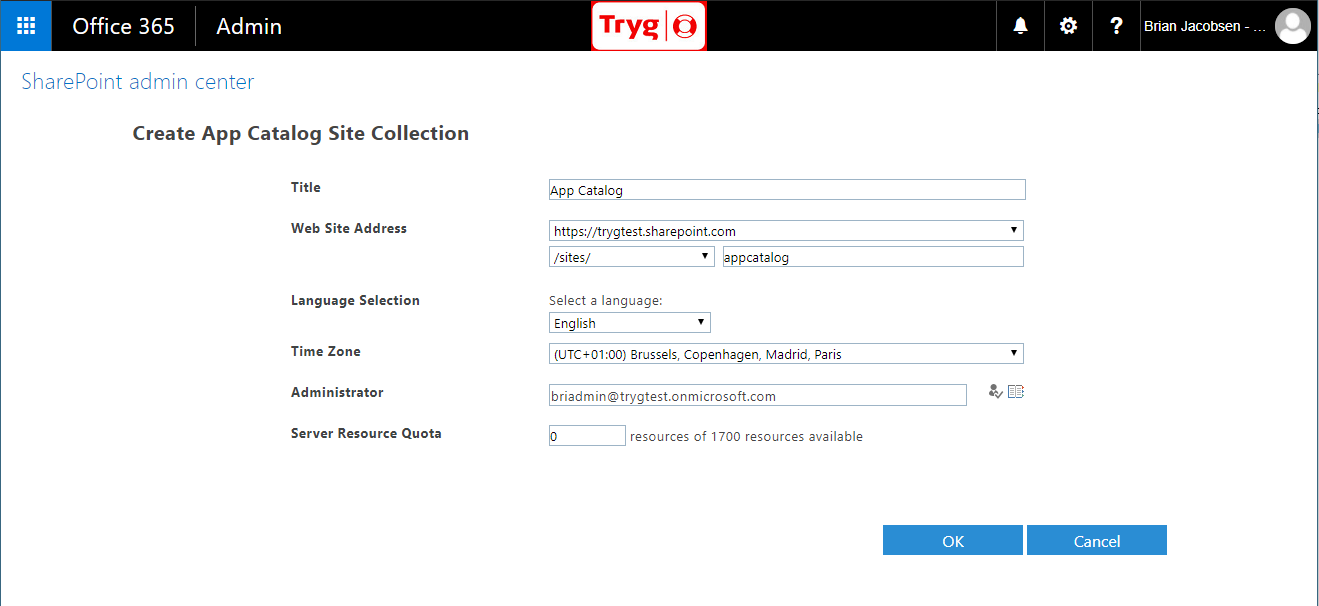
* Open the Office 365 Admin Center with a global admin
* Open the SharePoint admin center
* Select “apps”



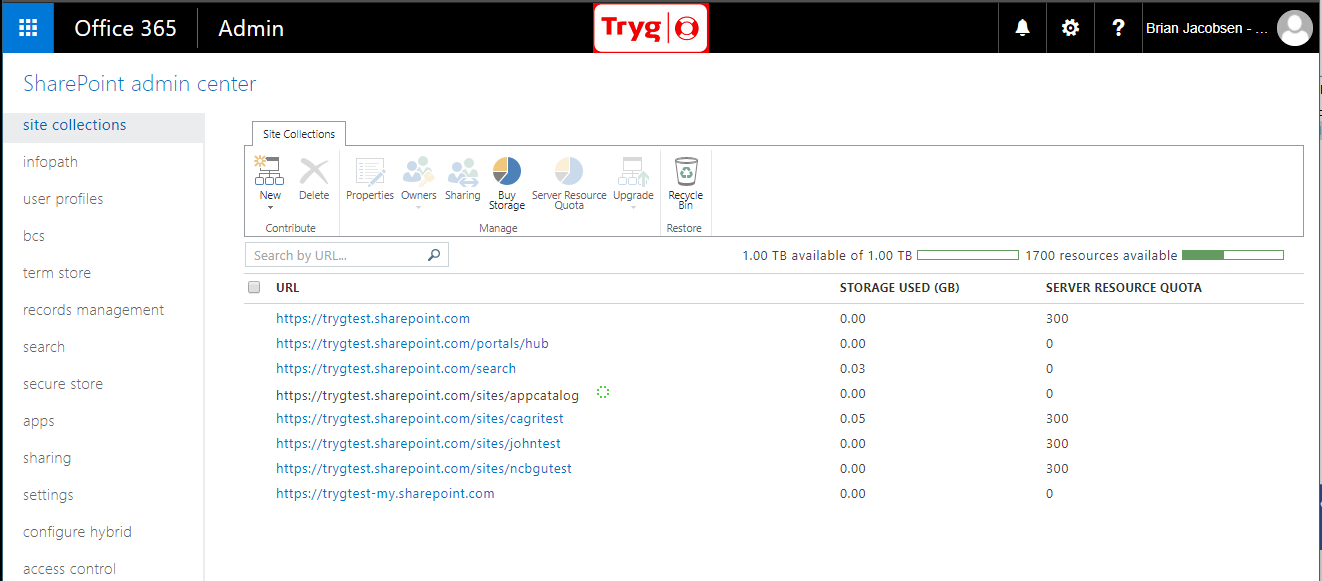
* Select “App Catalog”



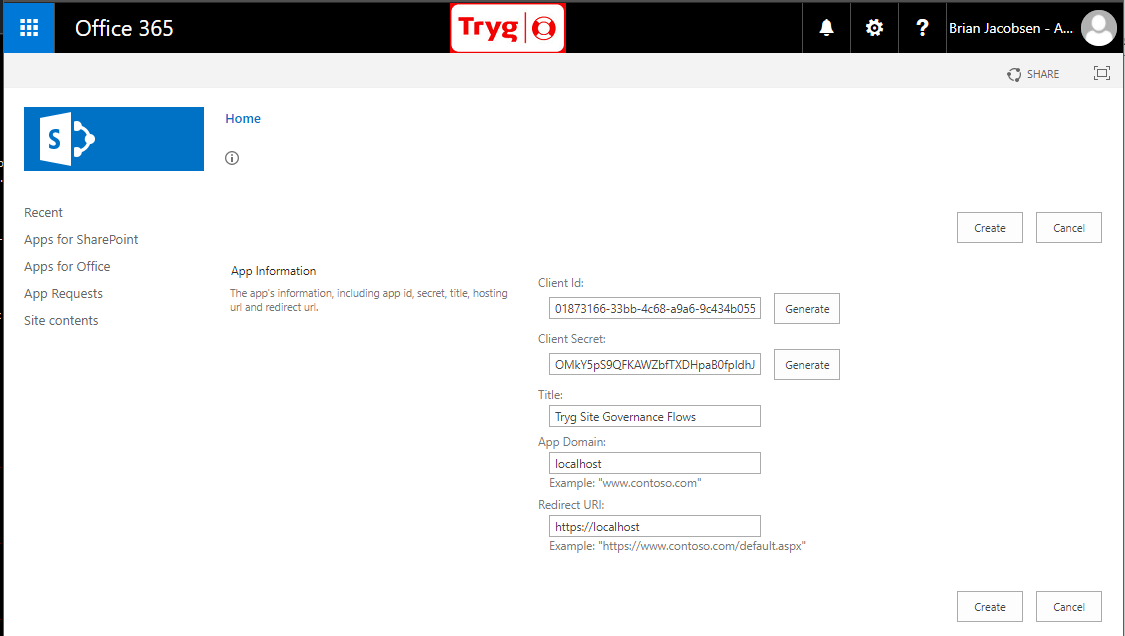
* If the App Catalog doesn’t exist, then create a new as per the CIL documentation



* Wait until the app catalog site is created (if creating it)

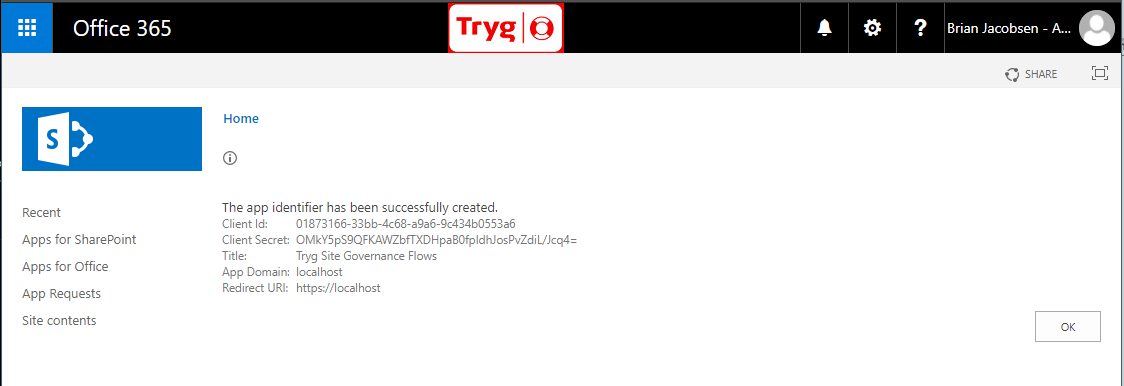


* Open <https://tryg.sharepoint.com/sites/apps/_layouts/15/appregnew.aspx> in the browser
* Select “Generate” at the Client Id (old name for AppId)
* Select “Generate” at the Client Secret (old name for AppSecret)
* Enter “Tryg Site Governance Flows” in the title
* Enter “localhost” as App Domain (not used)
* Enter “https://localhost” as Redirect Url (not used)
* Select Create

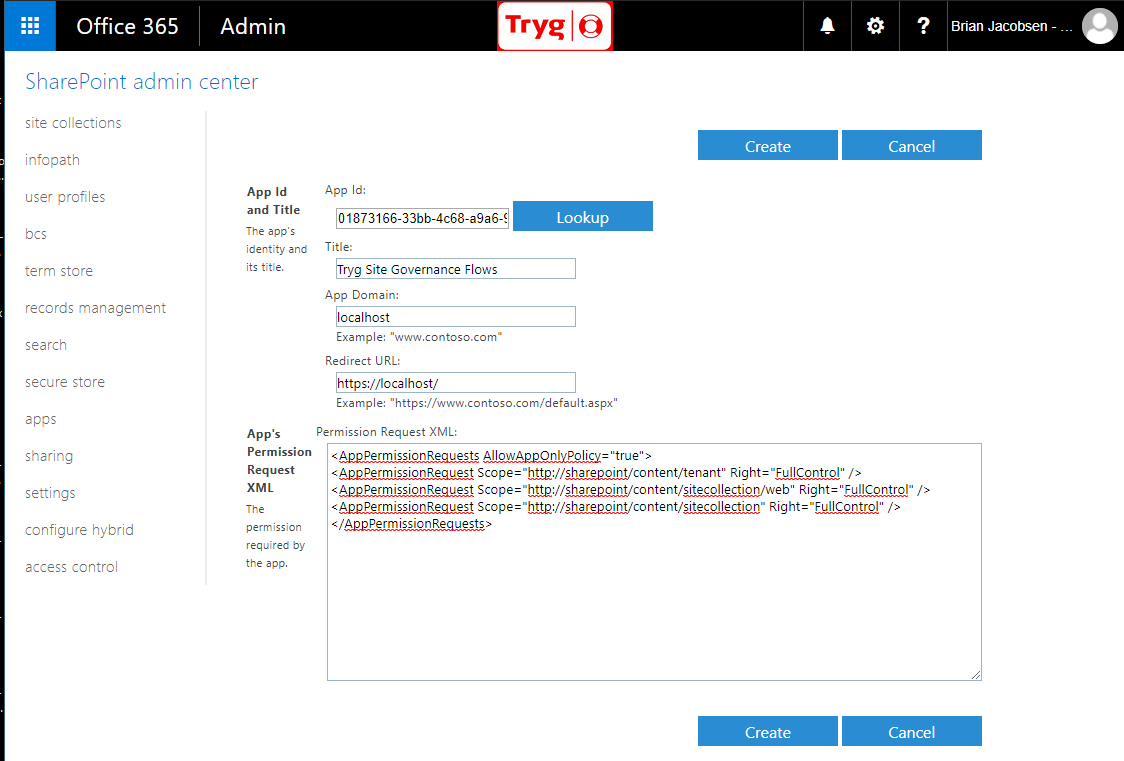


* Store the App ID and App Secret in the CIL (IMPORTANT – Only location to get the AppSecret)
* Set the expiration date in the CIL to be 12 months from todays date

|  |
| --- |
| The app identifier has been successfully created.  Client Id: 01873166-33bb-4c68-a9a6-9c434b0553a6  Client Secret: OMkY5pS9QFKAWZbfTXDHpaB0fpIdhJosPvZdiL/Jcq4=  Title: Tryg Site Governance Flows  App Domain: localhost  Redirect URI: <https://localhost> |



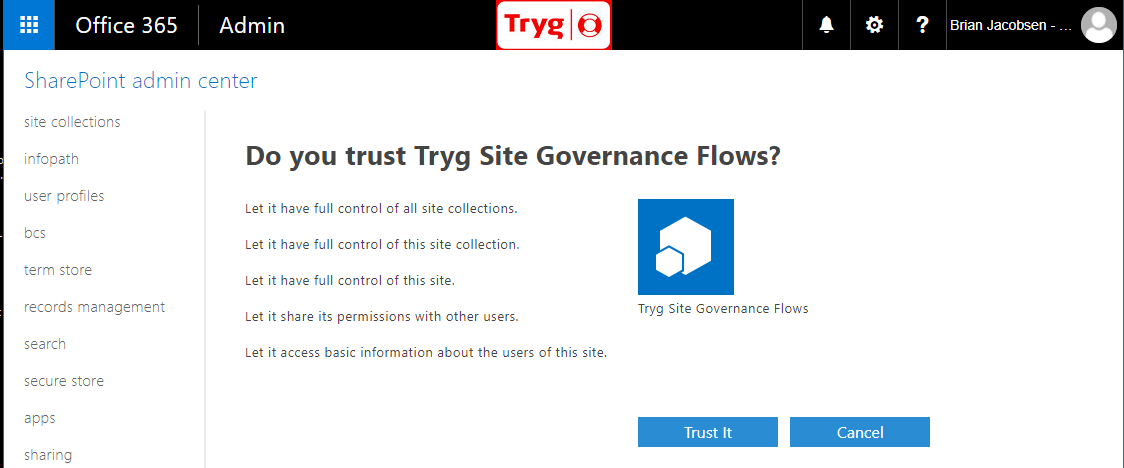
* Open the following link https://***tryg***-admin.sharepoint.com/\_layouts/15/appinv.aspx
* Enter the AppId in the AppId box, and select “Lookup”



* Enter the following in the App Permissions Request XML, which will grant the AppId/AppSecret combination site collection administrative permissions across the full tenant

|  |
| --- |
| <AppPermissionRequests AllowAppOnlyPolicy="true">  <AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="FullControl" />  <AppPermissionRequest Scope="http://sharepoint/content/sitecollection/web" Right="FullControl" />  <AppPermissionRequest Scope="http://sharepoint/content/sitecollection" Right="FullControl" />  </AppPermissionRequests> |

* Select “Trust It”



# Deploy Custom Services and Azure Resources

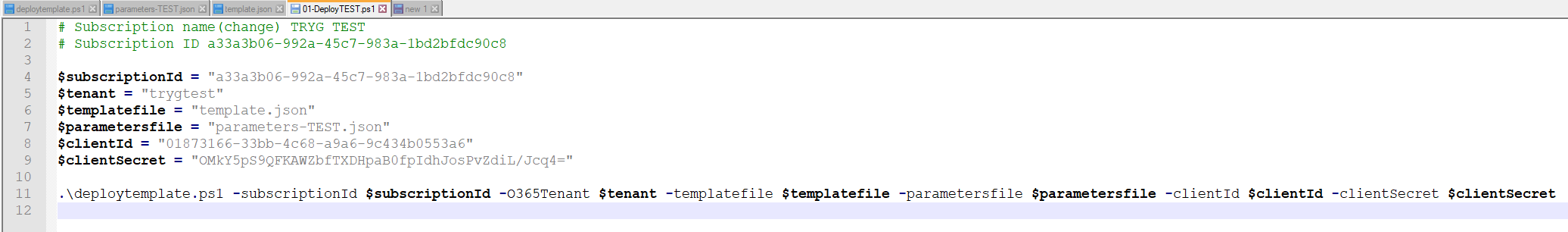
## Deploy the REST Service

The REST service is a custom support service, which will configure the SPO sites in areas where MS Flow does not have standard actions or connectors.

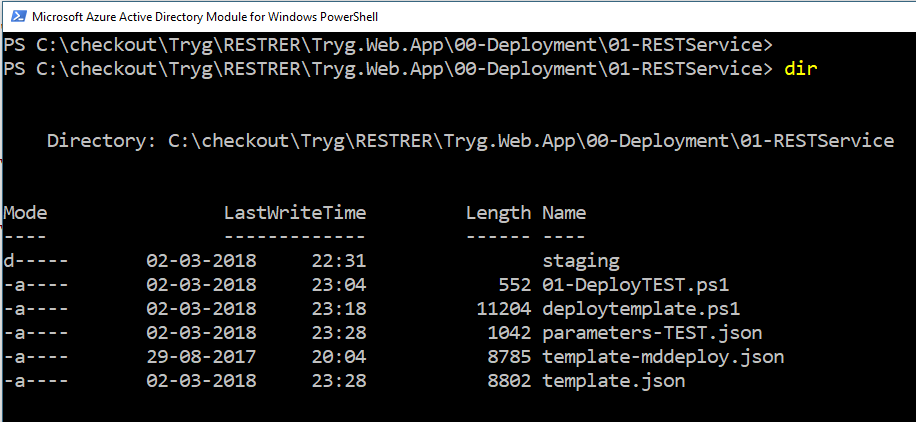
This is called through an HTTPS connection with a preshared key.

The configuration is documented in the CIL.

* Update the “01-Deploy***ENV***.ps1” script with
  + Azure subscription Id
  + ClientId (AppId created in previous step)
  + ClientSecret (AppSecret created in previous step)



* Open a AAD PowerShell prompt
* Run the “01-DeployTEST.ps1” to deploy to Azure
* Enter the credentials of an account which has at least Contributor permissions in the Azure Resource Group (see CIL for naming)

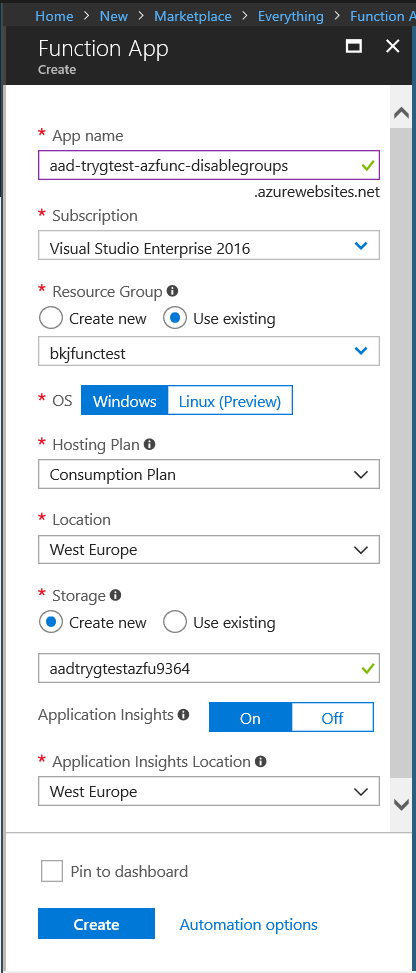


## Deploy Azure Function

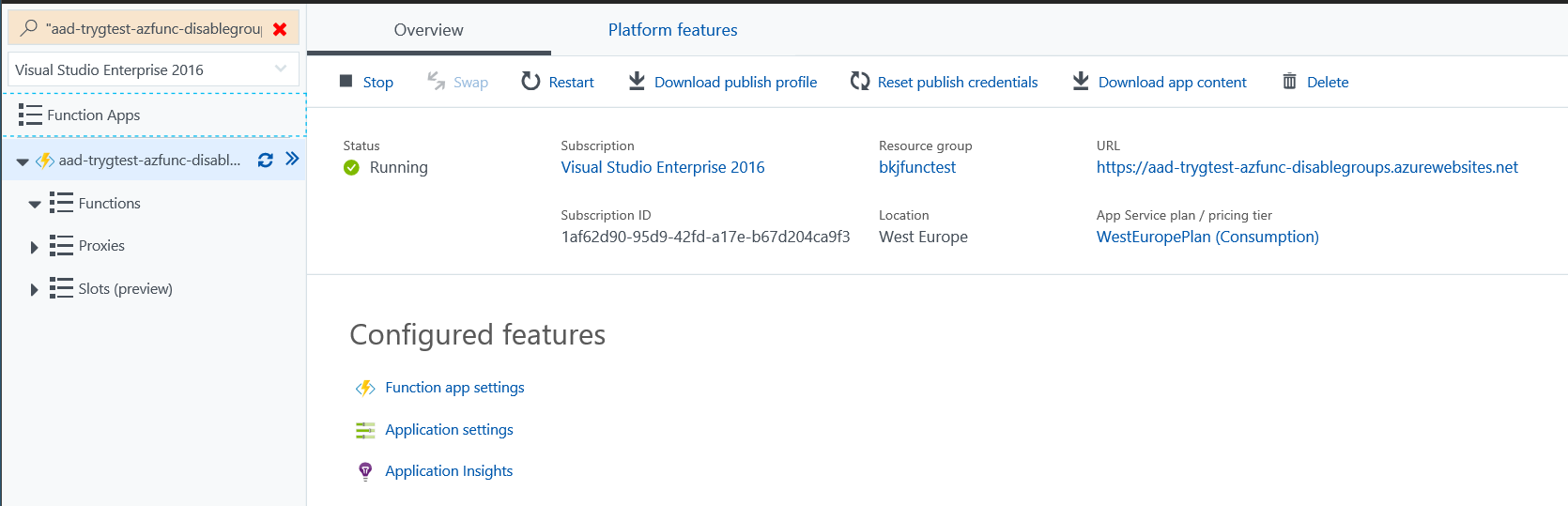
The Azure Function is created to utilize PowerShell to configure the guest access to individual Office 365 Groups.

This will be called from the MS Flow workflow outlined below.

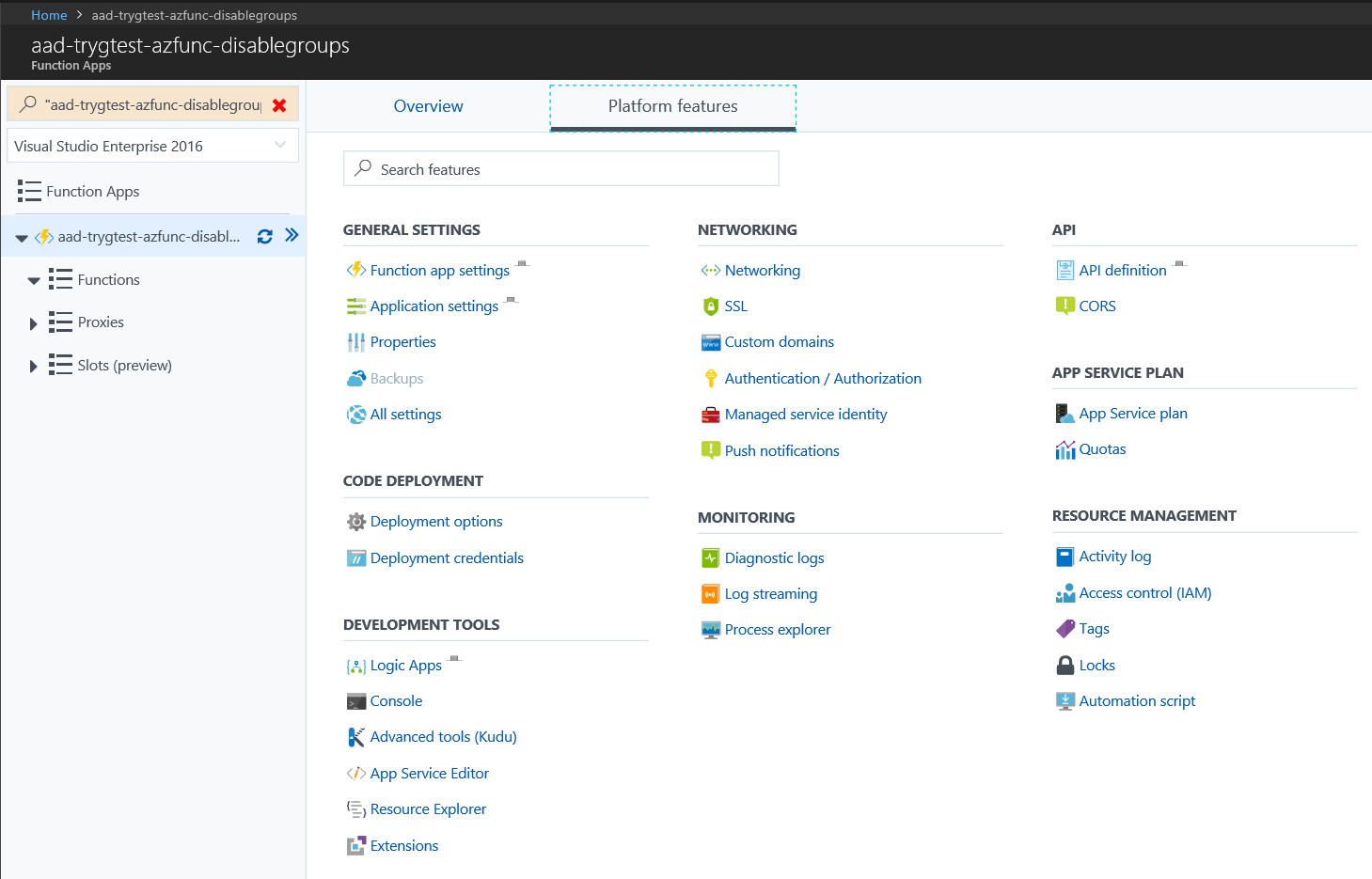
* Open the Azure Portal (https://portal.azure.com) with a minimum of Contributor permissions in the resource groups which is used for deployment – IMPORTANT: USE CHROME
* Create a new “Function App”
* Configure the Azure Function as per the CIL



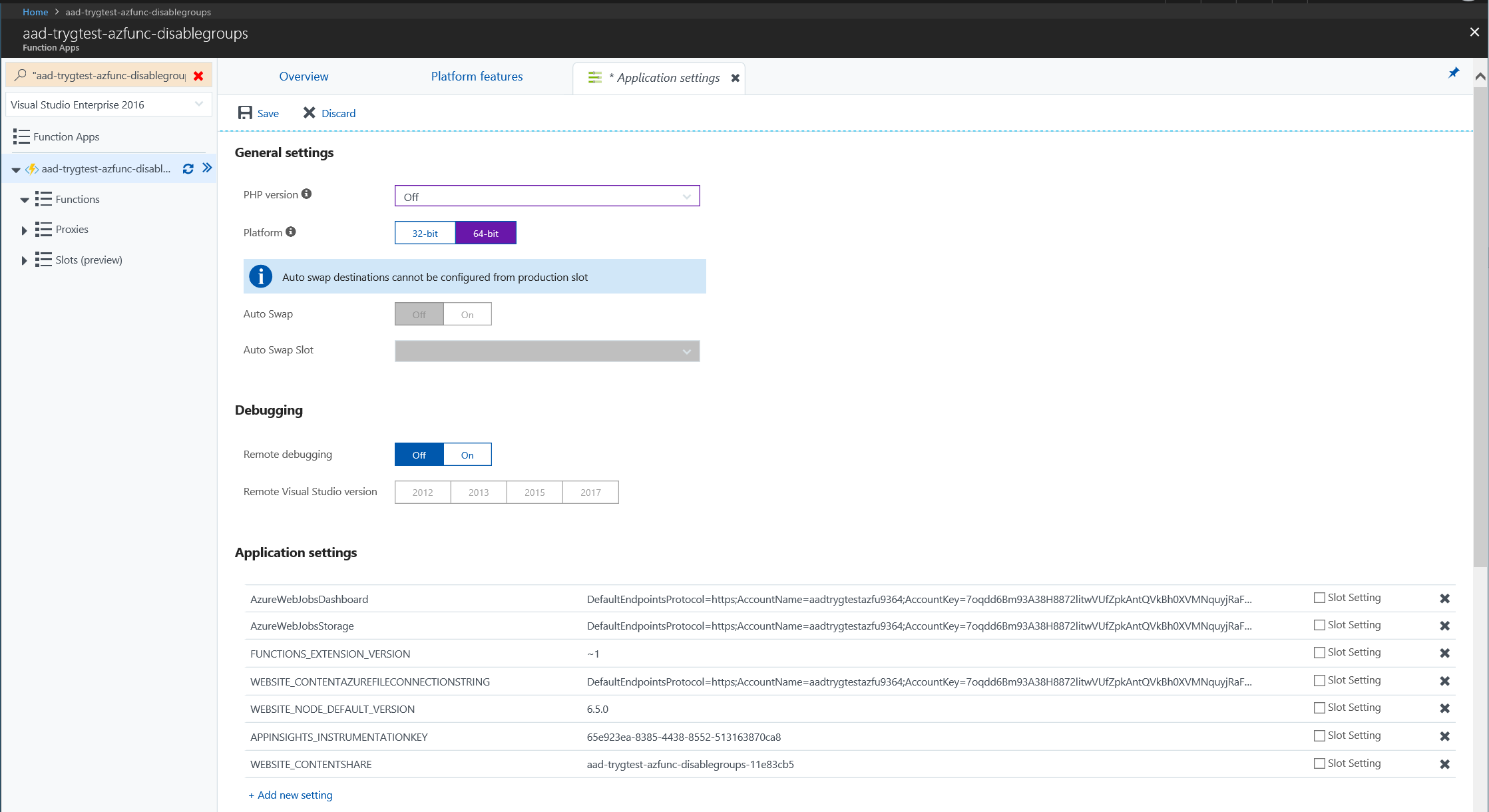
* Select “Create”
* Open the resource when the Azure Function is created
* Select “Platform Features”



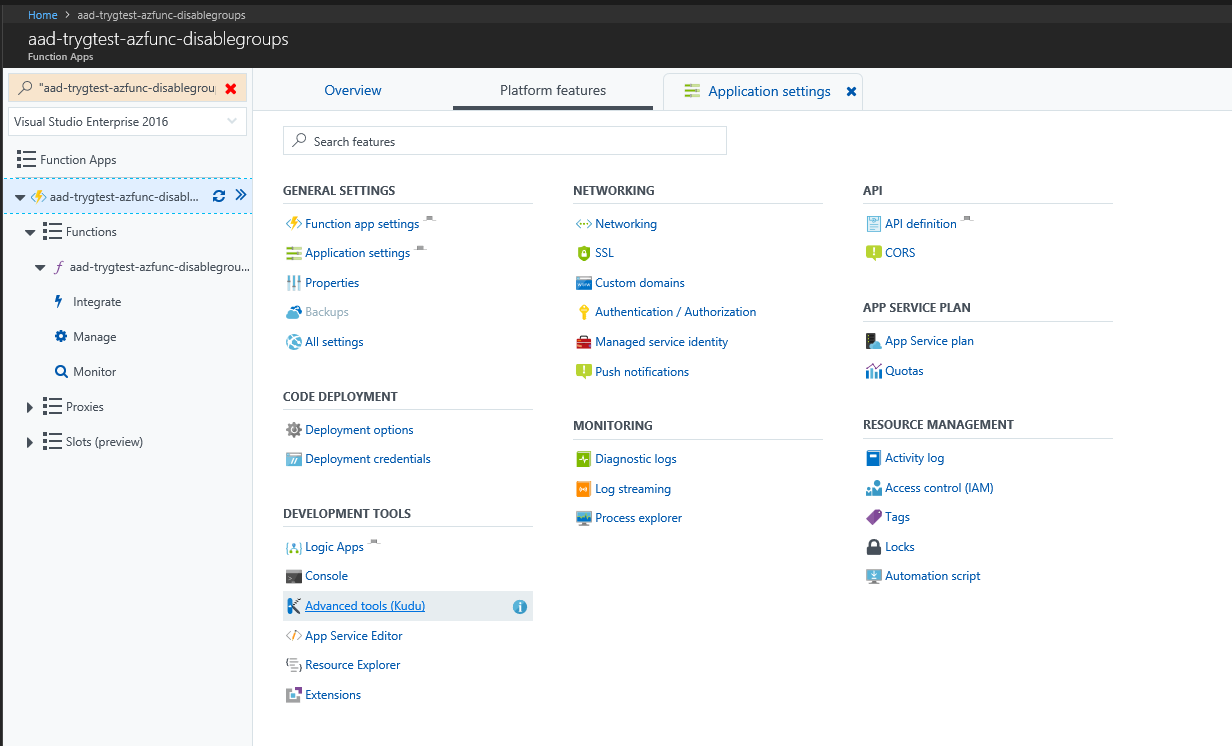
* Select “Application settings”



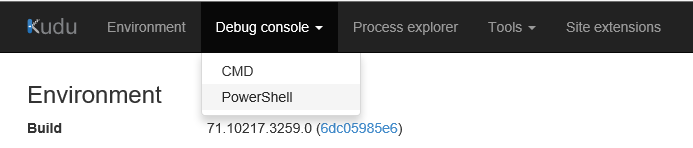
* Change the “PHP Version” to “Off”
* Change the platform to “64-bit”
* Add the application settings outlined in the CIL
* Select “Save”



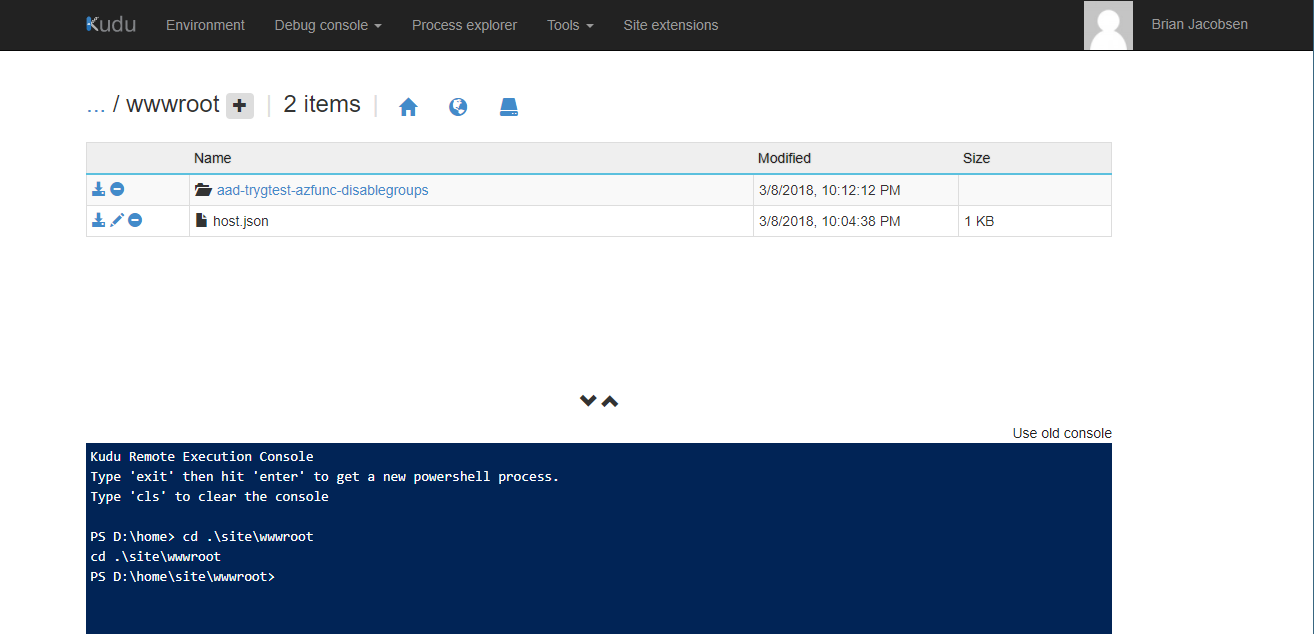
* Select the “Advanced tools (Kudu)” in the platform features



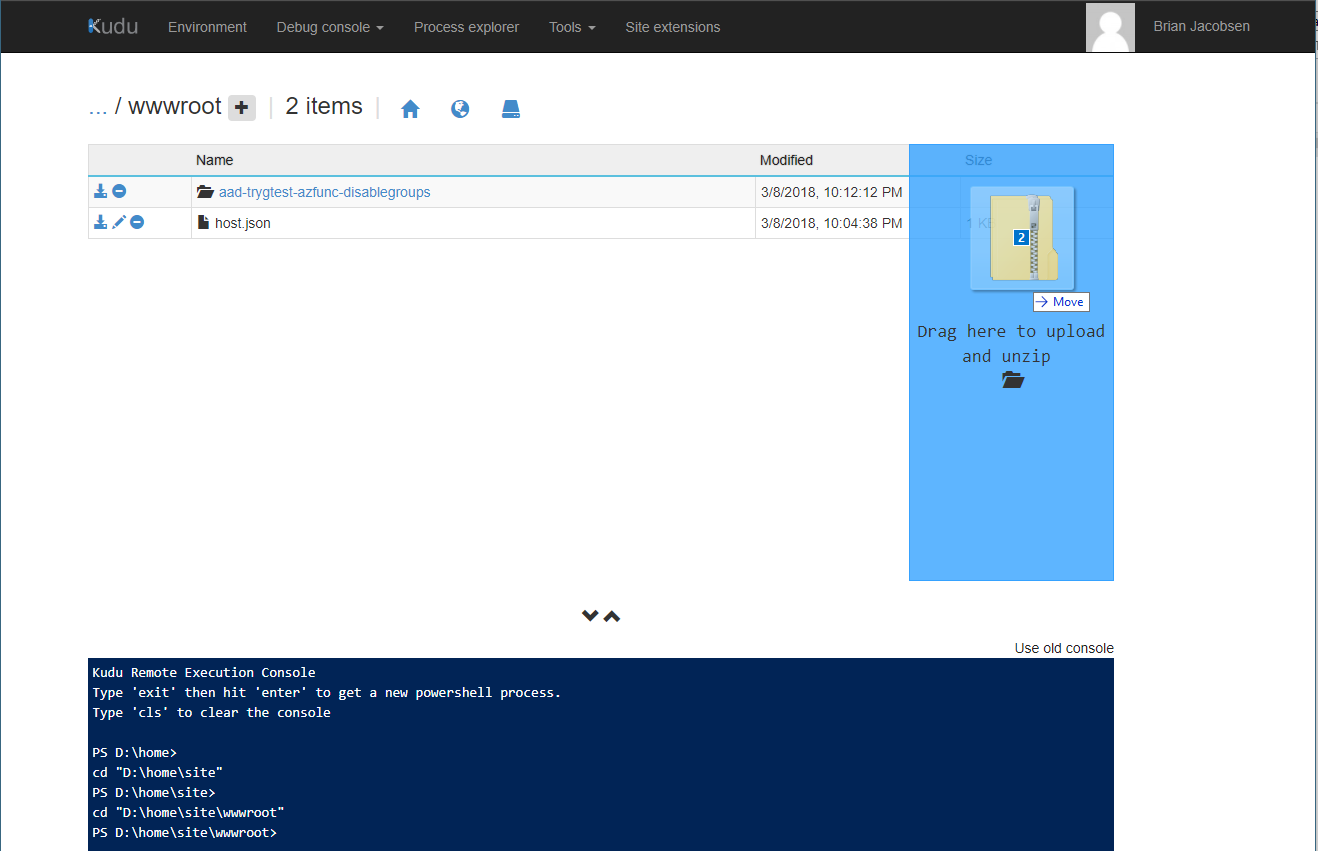
* Select the PowerShell prompt



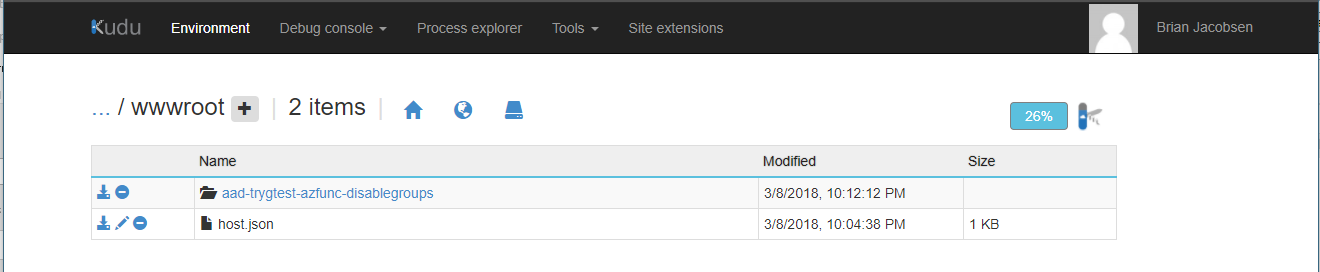
* Write “cd .\site\wwwroot”



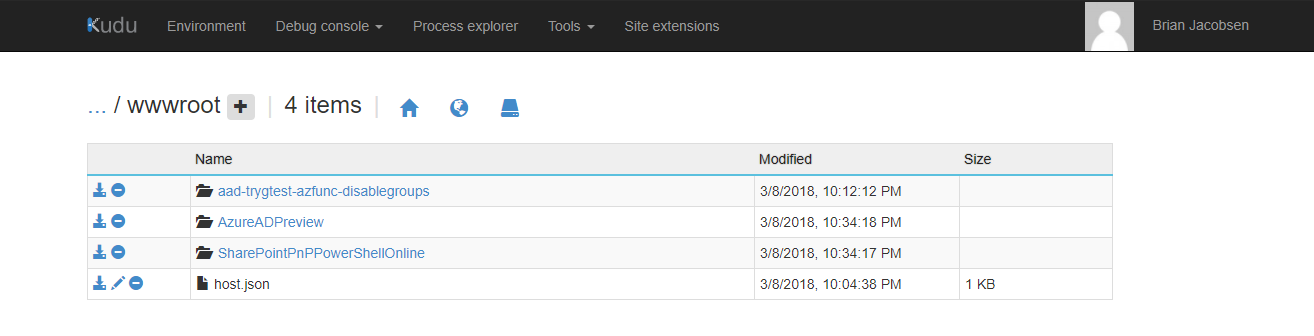
* Drag and drop the AzureADPreview.zip and SharePointPnPPowerShellOnline.zip into the wwwroot location (note must be dropped on the blue box on the right hand side)



* The progress is only shown in Chrome, not IE or Edge



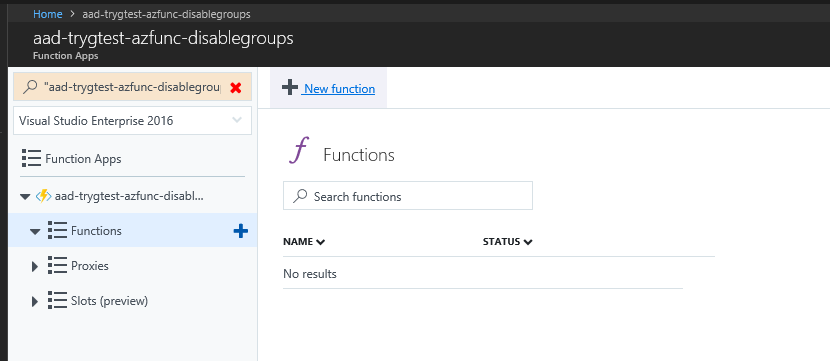
* Wait until the upload is completed (takes a while)



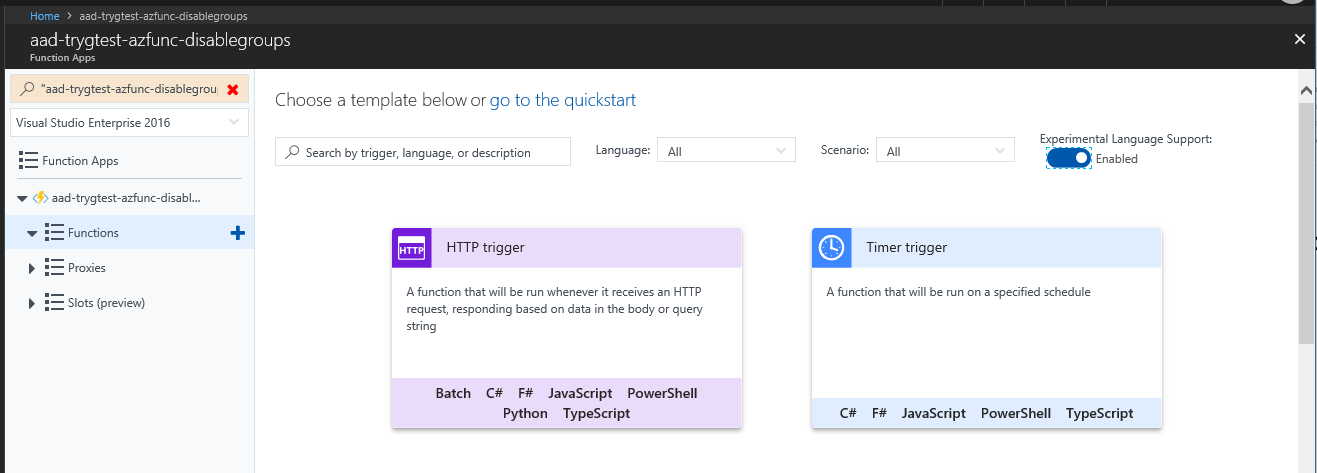
#### Azure Function: Disable External Guests

The Azure Function for disabling external guests in an Office 365 Group is added by the below steps.

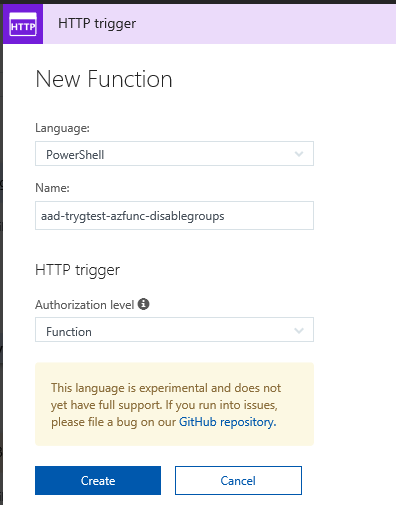
* Select the “New Function”



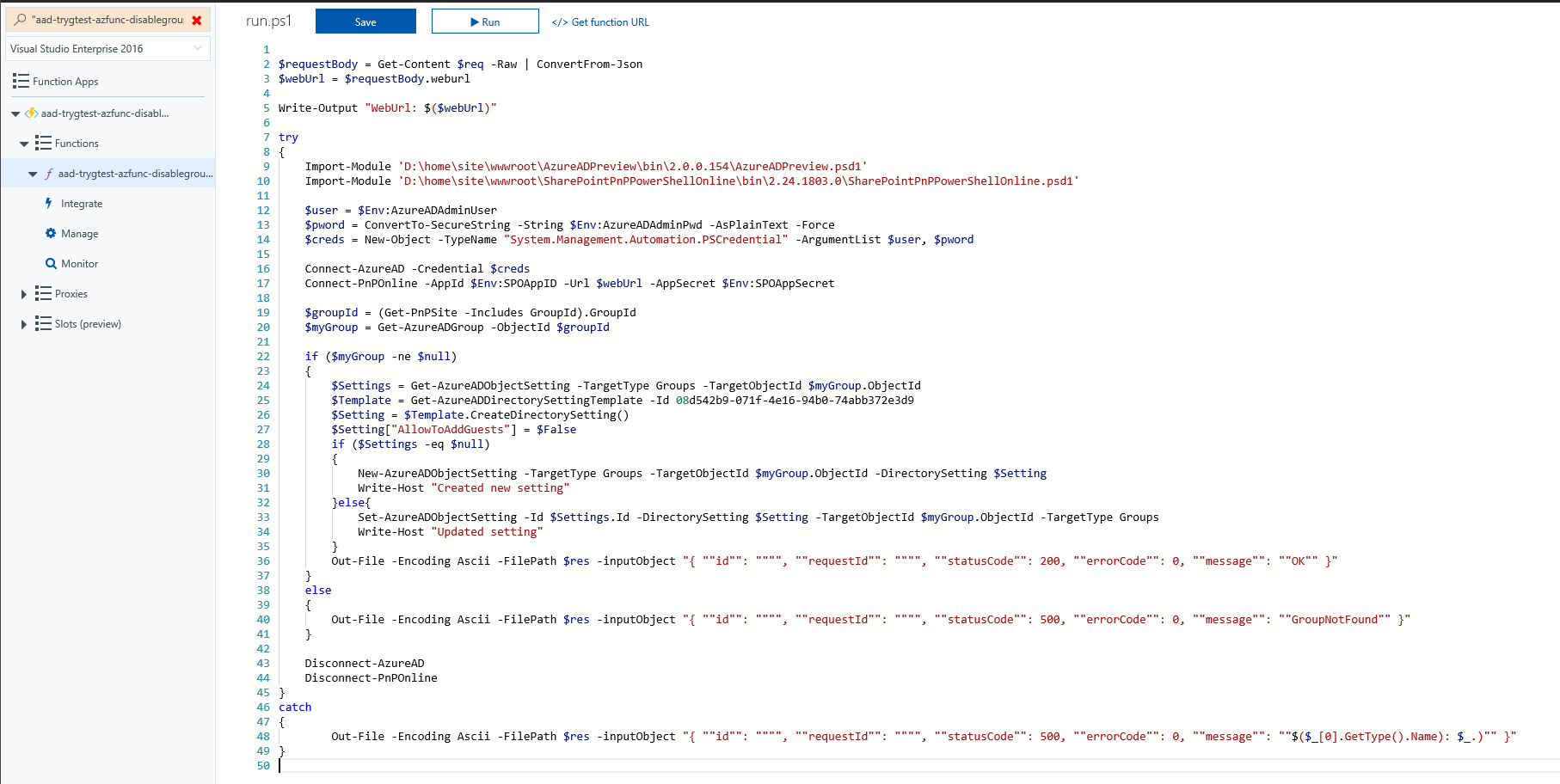
* Enable Experimental Language Support



* Select the “HTTP Trigger”
* Select language as PowerShell
* Configure the trigger as per CIL



* Paste the PowerShell code into the code window as per the CIL and press Save



* Select the “Get Function URL” and update the CIL

#### New azure function for set default audit log folder

The Azure Function for setting the audit log overflow folder is added by the below steps.

* Select the “New Function”
* Add the “Set Audit Log Path” Azure Function (see CIL)
* Enable Experimental Language Support
* Select the “HTTP Trigger”
* Select language as PowerShell
* Configure the trigger as per CIL
* Paste the PowerShell code into the code window as per the CIL and press Save
* Select the “Get Function URL” and update the CIL

#### New azure function for Scheduled Site Check Function

The Azure Function for perform a scheduled check for sites where the MS Flow call was failing in the site script, is added by the below steps.

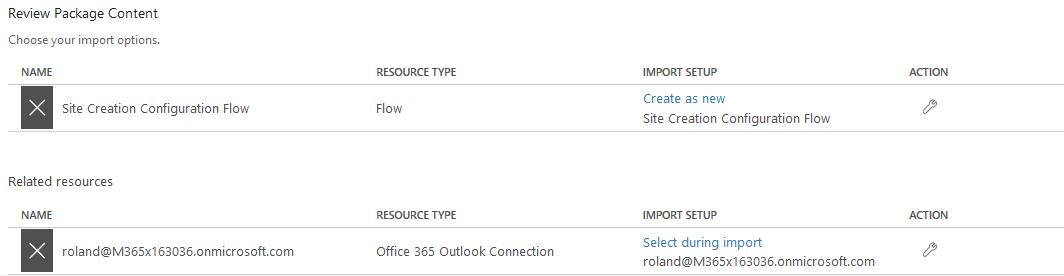
* Select the “New Function”
* Add the “Set Audit Log Path” Azure Function (see CIL)
* Enable Experimental Language Support
* Select the “Timer Trigger”
* Select language as PowerShell
* Configure the trigger as per CIL
  + Remember to set the schedule
* Paste the PowerShell code into the code window as per the CIL and press Save

## Deploy MS Flow Workflow

The Microsoft Flow must be imported in the MS Flow interface as the FLOW ACCOUNT

* Log into the Office 365 portal as the MS Flow Account (as per CIL)
* Select “Flow”
* Select “My Flows”
* Select “Import Flow”
* Select the MS Flow Package
* Select “Update” for first import setting and select “Create as new” form dropdown

Select “Update” for second import setting and select your account form available (note: if not available to select your flow account, then create new account in there with resource type “Office 365 Outlook Connection”, enter your flow account credentials)



* Update the following settings as per CIL
  + URL for REST Service
  + URL for Azure Function (this URL is created when the Azure Function is created)
  + Preshared Key
* Save the MS Flow
* Edit the MS Flow
* Copy the HTTP Trigger URL and update the CIL
* Add additional owners to the MS Flow as per the CIL

## Deploy SharePoint Site Script, Site Design and Theme

The deployment of the site script and site design is used to add functionality to a new site when that is created through the SharePoint Tile in Office 365 (Create Site)

The deployment of the theme (branding and colors) is used to provide a Tryg theme for the new team sites.

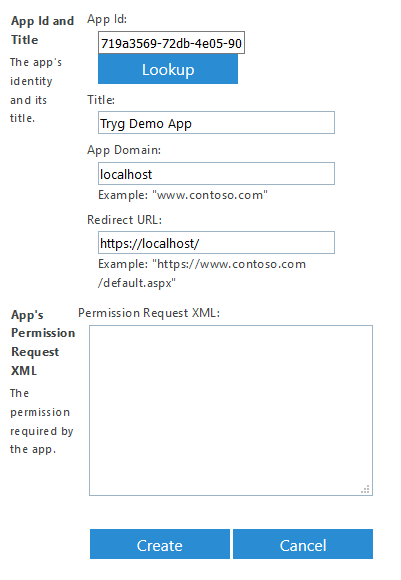
The site script is added as a default script on the standard team site template.

* Open a PowerShell prompt as a Windows Administrator
* If the “SharePointPnPPowerShellOnline” module isn’t installed, then execute
  + Install-Module SharePointPnPPowerShellOnline
* If the “SharePointPnPPowerShellOnline” module is installed, then execute
  + Update-Module SharePointPnPPowerShellOnline
* Update the “Apply-Configuration.ps1” script with the AppId and AppSecret credentials created previously
* Update the “SiteScript.json” script with the URL to the MS Flow created previously
* Execute the “Apply-Configuration.ps1” script

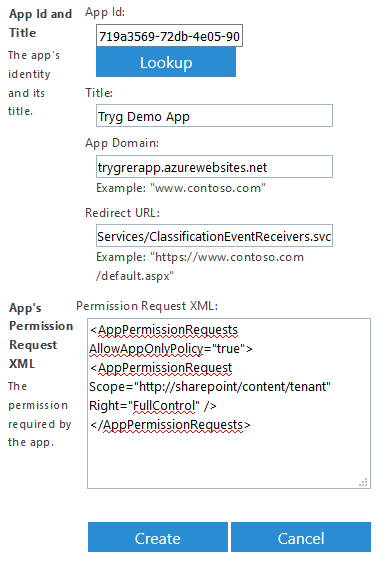
# Release 2

## Update SPO App permissions

* Open the following link https://***tryg***-admin.sharepoint.com/\_layouts/15/appinv.aspx
* Enter initial AppId (see CIL) in the AppId box, and select “Lookup”



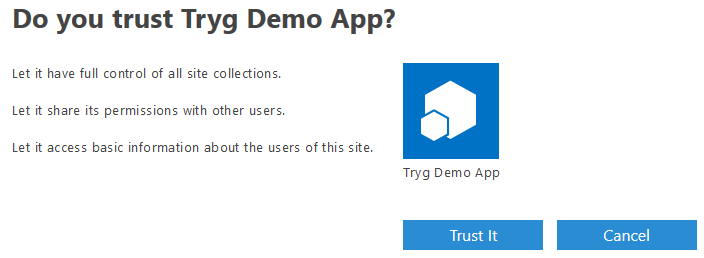
* Change App Domain to Azure web app as per CIL
* Change Redirect Url to “https://” +Azure web app as per CIL + “/Services/ClassificationEventReceivers.svc”



* Enter the following in the App Permissions Request XML, which will grant the AppId/AppSecret combination site collection administrative permissions across the full tenant

|  |
| --- |
| <AppPermissionRequests AllowAppOnlyPolicy="true">  <AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="FullControl" />  </AppPermissionRequests> |

* Select “Trust It”

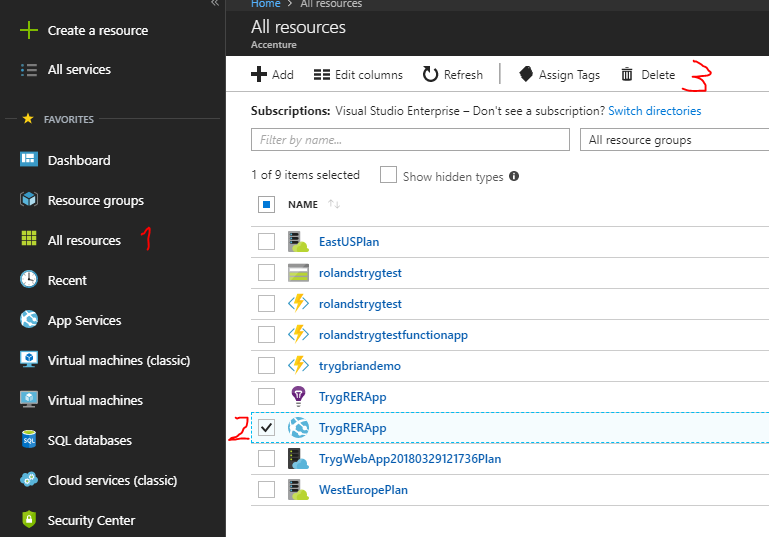


## Update the REST Service

Azure app service must be deleted and then re-deployed by running script.

To delete azure app service, follow these steps:

1. Go to <http://portal.azure.com/>
2. Log in with tryg admin account
3. Go to All resources
4. Check app service “nespoappsrv01”
5. Press “Delete”



To deploy the Rest Service, follow instructions in section 3.1

## Changed Azure Functions

### Update azure function: Disable External Sharing

* Select azure function for disabling external sharing as per CIL
* Replace code with code in CIL

### Update azure function: Set Log Path

* Select azure function for setting log path as per CIL
* Replace code with code in CIL

### Update azure function: Scheduled Site Configuration

* Select azure function for scheduled site configuration as per CIL
* Replace code with code in CIL

### New azure function: Set Classification

The Azure Function for perform a scheduled check for sites where the MS Flow call was failing in the site script, is added by the below steps.

* Select the “New Function”
* Add the “Set Classification” Azure Function (see CIL)
* Enable Experimental Language Support
* Select the “HTTP Trigger”
* Select language as PowerShell
* Configure the trigger as per CIL
* Paste the PowerShell code into the code window as per the CIL and press Save
* Select the “Get Function URL” and update the CIL

### New azure function: Get Owner Emails

The Azure Function for perform a scheduled check for sites where the MS Flow call was failing in the site script, is added by the below steps.

* Select the “New Function”
* Add the “Get Owner Emails” Azure Function (see CIL)
* Enable Experimental Language Support
* Select the “HTTP Trigger”
* Select language as PowerShell
* Configure the trigger as per CIL
* Paste the PowerShell code into the code window as per the CIL and press Save
* Select the “Get Function URL” and update the CIL

### Update application settings

Update application settings as per CIL

## Changed MS Flow

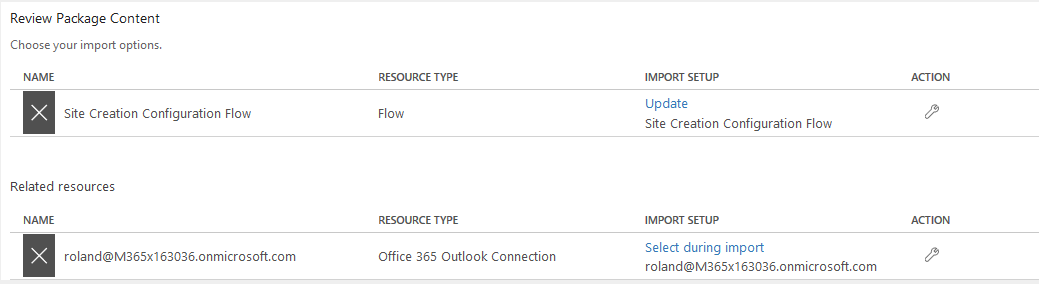
Update of MS Flow is required.

To update MS Flow

Don’t forget to update variables in flow as per CIL settings:

* Log into the Office 365 portal as the MS Flow Account (as per CIL)
* Select “Flow”
* Select “My Flows”
* Select “Import”
* Select the MS Flow Package
* Select “Update” for first import setting and select already existing flow named “Site Creation Configuration Flow”

Click on “Select during import” for second import setting and select your account form available



* Click “Import”
* Update the following settings as per CIL
  + URL for REST Service
  + URL for Azure Function to Disable guest access (this URL is created when the Azure Function is created)
  + URL for Azure Function to Set audit log path (this URL is created when the Azure Function is created)
  + URL for Azure Function to Get owner emails (this URL is created when the Azure Function is created)
  + Preshared Key
* Save the MS Flow