sko

SPOCPI



Deployment Guide

Prepared for

Shell Information Technology International BV

3-Jul-2020

Version 1.0 Draft

Prepared by

**Shell Search Coe Team**

Prior to the parties indicating final agreement by signing a Work Order, the information contained in this document represents the current view of Microsoft on the issues discussed as of the date of publication and is subject to change. Furthermore, prior to the signing of the Work Order, this document should not be interpreted as an invitation to contract or a commitment on the part of Microsoft. After the Work Order has been signed, changes to this document will be managed through the Change Management Process described in this document.

IF THIS DOCUMENT IS INCORPORATED BY REFERENCE INTO A WORK ORDER, ALL WARRANTIES APPLICABLE TO THE WORK ORDER APPLY TO THIS DOCUMENT. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

The descriptions of other companies’ products in this document, if any, are provided solely as a convenience to aid understanding and should not be considered authoritative or an endorsement by Microsoft. For authoritative descriptions of any non-Microsoft products described herein, please consult the products’ respective manufacturers. © 2014 Microsoft. All rights reserved. Any use or distribution of these materials without the express authorization of Microsoft is strictly prohibited.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft in the United States and/or other countries.

Contents

[1 Objective 4](#_Toc37790311)

[2 Deployment Package 4](#_Toc37790312)

[3 Prerequisites 6](#_Toc37790313)

[3.1 User Machine prerequisites 6](#_Toc37790314)

[3.2 Prerequisites 6](#_Toc37790315)

[3.3 Prepare deployment workspace 6](#_Toc37790316)

[3.4 Update Parameters 6](#_Toc37790317)

[4 Deployment Steps 8](#_Toc37790318)

[5 Post Deployment Validation 9](#_Toc37790319)

[6 Maintenance activities 11](#_Toc37790320)

[7 Miscellaneous 11](#_Toc37790321)

[7.1 Create AAD Application 11](#_Toc37790329)

# Objective

SPOCPI Deployment guide is intended to provide the deployment steps that includes:

* What to expect from the deployment package?
* Prerequisites.
* Pre-deployment activities (includes configuration changes and parameters updates).
* Deployment steps.
* Post Deployment Validation steps.

# Deployment Package

SDU deployment package contains following files.

|  |  |  |
| --- | --- | --- |
| # | File | Purpose |
| 1 | azuredeploy.json | Contains ARM Template for defining the Azure resources to be created. |
| 2 | azuredeploy.parameters.json | Contains the parameters for azure deployment as well configuration storage table entries. |
| 3 | spocpimaster.ps1 | Master script file that is responsible for executing the below script files in an order. |
| 3 | azuredeploy.ps1 | Contains ARM templates for the cloud resources that needs to be deployed in the resource group |
| 4 | azlogin.ps1 | Standalone script used to login and set the subscription that is mentioned in parameters file. |
| 5 | codepublish.ps1 | Standalone script used to clean and build SDU solution and generate the below zip files for each output.   * Shell.SPOCPI.WebHooksManager.UI.zip * Shell.SPOCPI.WebHooksManager.WebJob.zip * Shell.SPOCPI.NotificationReceiver.FunctionApp.zip * Shell.SPOCPI.ChangeProcessor.FunctionApp.zip * Shell.SPOCPI.ChangeProcessor.WebJob.zip * Shell.SPOCPI.PopulateTracking.FunctionApp.zip |
| 6 | codedeploy.ps1 | Standalone script used to deploy the zip files generated above to cloud resources like function app, webapp, Api App etc.  **Note:** services.csv file present under deploy folder has the mapping configured for each webapp/function app against the zip file. |
| 7 | createappsettings.ps1 | Standalone script used to set app settings for function app/webapp. For each function app/webapp, the app settings data is present in appsettings folder in deploy directory.  Below are the files present in appsettings folder:   * spocpiwebhooksmanagerapp.appsettings.json * spocpinotificationreceiver.appsettings.json * spocpichangeprocessor.appsettings.json * spocpichangeprocessorapp.appsettings.json * spocpipopulatetracking.appsettings.json |
| 8 | configurekeyvault.ps1 | Standalone script used to create secrets in KeyVault and grant Managed Service Identity access to function app/webapp.  **Note:**   * Function names whose keys needs to be stored in KeyVault are configured in functions.csv file under keyvault folder. * Function Apps/web apps that needs access to keyvault are configured in keyvaultappprincipals.csv file under keyvault folder. |
| 9 | configuresearch.ps1 | Standalone script used to configure search, that includes creating:   1. Index 2. Indexer 3. Data source   **Note:**  Index, indexer and data source that needs to be created are present in search folder in deploy directory. |
| 10 | storagedeploy.ps1 | Standalone script used to configure the storage accounts, that includes creating:   * Web Hooks storage account Tables   1. Configuration   2. Subscriptions * Doc Track storage account Tables   1. DocumentTracking   2. DriveDelta   3. NotificationStorage   The script also adds configuration entries into Configuration table. Configuration data is read from **Configuration.typed.csv** present in tables folder. |
| 11 | restartservices.ps1 | Standalone script used to restart function app/webapp.  **Note:**  List of function app/webapp that needs to be restarted are configured in services.csv file under deploy folder. |
| 12 | commonhelpers.psm1 | Powershell module file that contains reusable functions used by other scripts. |

# Prerequisites

# User Machine prerequisites

1. Below are the pre-requisites for running the scripts on the user’s machine:

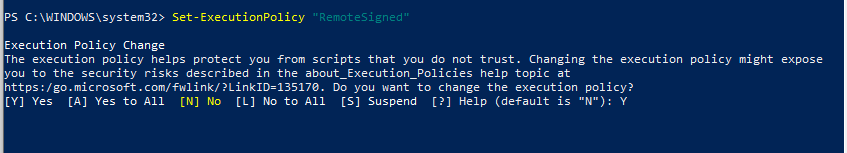
* Windows PowerShell
* **For Windows :** [5.1 or higher](https://docs.microsoft.com/en-us/skypeforbusiness/set-up-your-computer-for-windows-powershell/download-and-install-windows-powershell-5-1)
* **All Platforms :** [PowerShell Core 6.x](https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell?view=powershell-6#powershell-core) and higher
* [Azure PowerShell Module](https://docs.microsoft.com/en-us/powershell/azure/install-az-ps?view=azps-2.8.0)
* [Azure CLI](https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest)

1. Restart **Windows PowerShell** after installing above pre-requisites
2. If the scripts are not allowed to execute on the machine, we can follow below steps to allow execution of the script:

* Unblock all PowerShell scripts and DLL files by unblocking files in **deploy folder** in Windows Explorer (right-click -> Properties -> checkmark: Unblock -> OK)
* Open PowerShell.exe in administrator mode
* Type the following command:

**Set-ExecutionPolicy “RemoteSigned”**

Type “Y” for yes to confirm.



# Prerequisites

1. Ensure that the account with which the deployment script is executed has atleast Contributor access on the subscription.

# Prepare deployment workspace

1. Get the latest SPOCPI package (either in a plain directory/as a compressed file [.zip]).
2. Copy/Unzip the package content to a directory named “**deploy**”.

**Note:** Name should be “**deploy**” as the directory name is being referred in deployment scripts.

1. Check the deploy directory has all the required files for the deployment. Refer [Deployment Package](#_Deployment_Package) for further details.

# Update Parameters

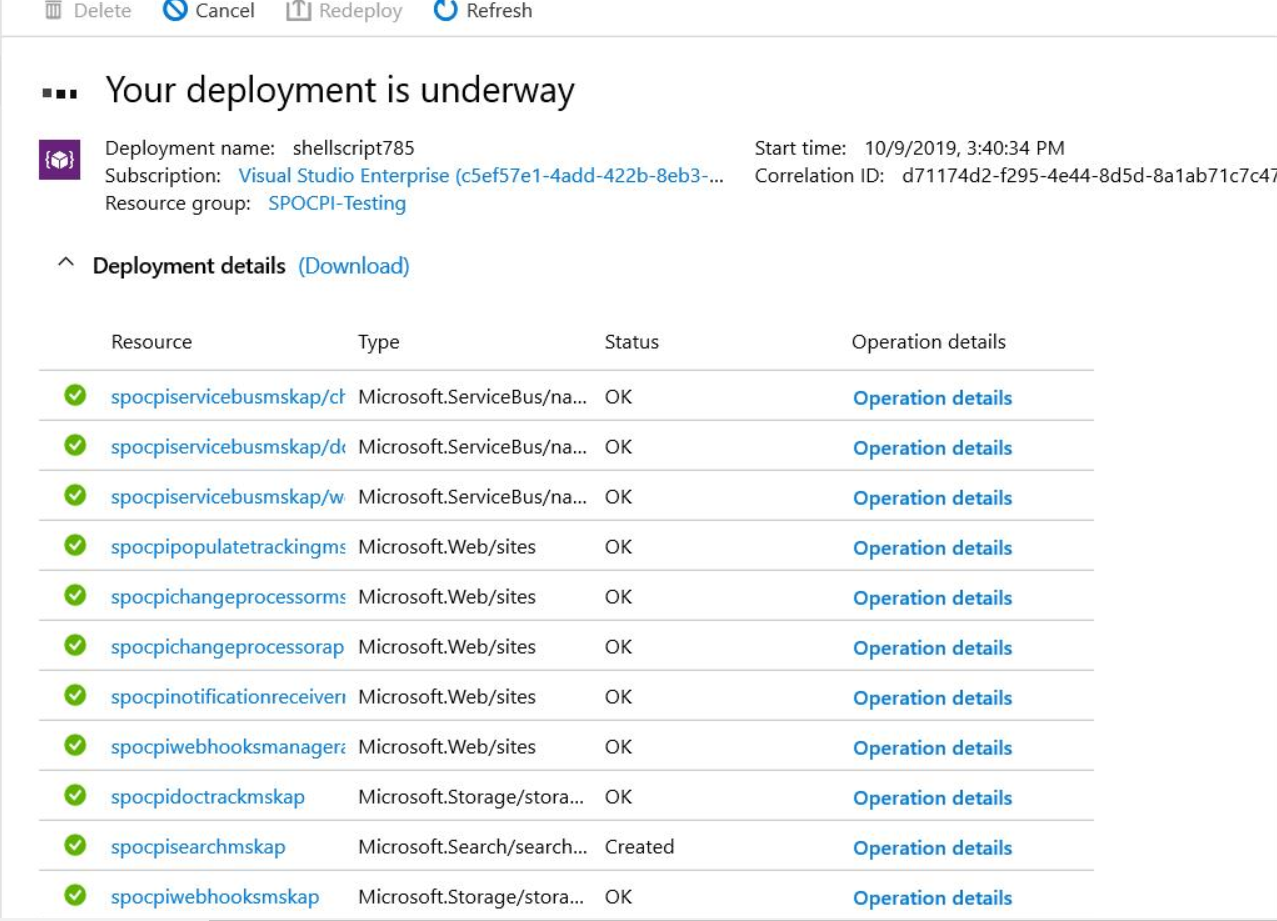
Parameters section in **azuredeploy.parameters.json** needs to be updated as per the deployment environment. Follow below steps.

* + 1. Open Windows Explorer and open the SPOCPI deployment workspace (**deploy** directory).
    2. Open “**azuredeploy.parameters.json**” in your preferred notepad editor.
    3. Find the property “**parameters**”
    4. Please refer below table for details of all parameters.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Parameter Name | Default Value | | Details |
| 1 | resourceGroupName |  | Azure resource group name | |
| 2 | subscriptionId |  | Azure subscription id | |
| 3 | tenantName |  | SharePoint tenant name | |
| 4 | environment |  | Environment name.  **Examples:**   |  |  | | --- | --- | | dev | essdev | | test | esstest | | uat | essuat | | production | essprod | | |
| 5 | location | westeurope | Location of the resource group. Should be westeurope by default. | |
| 6 | AADAppClientId |  | AAD App’s client id. This app should have permissions should have below permissions   1. Azure Active Directory Graph 🡺 Directory.ReadAll 2. Microsoft Graph 🡺 Sites.Read.All. | |
| 7 | AADAppClientSecret |  | AAD App’s client secret. | |
| 8 | storageaccountsku | Standard | Storage Pricing pricing tier | |
| 9 | servicebussku | Standard | Service Bus pricing tier | |
| 10 | appservicesku | Standard | App service pricing tier | |
| 11 | highconsumptionappservicesku | Standard | App service pricing tier (for high consumption apps like changeprocessor webjob) | |
| 12 | appServiceWorkerSize | 2 | App service worker size | |
| 13 | highconsumptionappserviceworkerSize | 2 | App service worker size (for high consumption apps) | |
| 14 | appserviceskuCode | S1 | App service Sku code | |
| 15 | highconsumptionappserviceskuCode | S1 | App service Sku code (for high consumption apps) | |
| 16 | redisCacheName | spocpirediscache | Redis cache name | |
| 17 | redisCacheSKU | Standard | Redis cache Sku code | |
| 18 | docTrackStorage | spocpidoctrack | Document tracking storage account name | |
| 19 | webHooksStorage | Spocpiwebhooks | Web Hooks storage account name | |
| 20 | webHooksStorageTableNames | "Configuration",  "Subscriptions" | Table names for webhooks storage | |
| 21 | docTrackStorageTableNames | "DocumentTracking","DriveDelta",  "NotificationStorage" | Table names for document tracking storage | |
| 22 | StorageAccountType | Standard\_ZRS | Storage account type | |
| 23 | changeprocessorFunctionApp | spocpichangeprocessor | Change processor function app name | |
| 24 | changeprocessorWebApp | spocpichangeprocessorapp | Change processor web app | |
| 25 | notificationReceiverFunctionApp | spocpinotificationreceiver | Notification receiver function app name | |
| 26 | populateTrackingFunctionApp | spocpipopulatetracking | Populate tracking function app name | |
| 27 | webHooksManagerWebApp | spocpiwebhooksmanagerapp | WebHooks manager web app name | |
| 28 | serviceBusNamespaceName | spocpiservicebus | Service Bus name | |
| 29 | changeprocessoutputqueue | changeprocessoutputqueue | Change process output queue name | |
| 30 | Webhooksnotificationqueue | webhooksnotificationqueue | Web hooks notification queue name | |
| 31 | doctrackqueue | doctrackqueue | Document tracking queue name | |
| 32 | SearchName | spocpisearch | Search service name | |
| 33 | keyVaultName | spocpikeyvault | Keyvault name | |

# Deployment Steps

1. Open Windows Powershell as Administrator
2. Navigate to the SPOCPI deploy folder
3. Execute **.\spocpimaster.ps1** command and login with your shellcorp2 account and wait for the script execution to complete
   1. Master script will execute below scripts in sequence order
      1. codepublish.ps1
      2. azuredeploy.ps1
      3. codedeploy.ps1
      4. configurekeyvault.ps1
      5. storagedeploy.ps1
      6. sanitizeappsettings.ps1
      7. createappsettings.ps1
      8. configuresearch.ps1
      9. restartservices.ps1
4. Navigate to the resource group to see if the execution status is Successful



1. After script is executed successfully, please collect the below logs generated by scripts and see if there are any errors logged
   1. spocpimaster\_DateTime.txt
   2. azuredeploy\_DateTime.txt
   3. codedeploy\_DateTime.txt
   4. configurekeyvault \_DateTime.txt
   5. storagedeploy\_DateTime.txt
   6. sanitizeappsettings\_DateTime.txt
   7. createappsettings \_DateTime.txt
   8. configuresearch\_DateTime.txt

# Post Deployment Validation

1. Navigate to the resource group and verify if all the resources are created successfully or not.

**Example**: If the environment name provided in the parameters file is msdev, then below resources would have been created by the script.

|  |  |  |
| --- | --- | --- |
| Sl.No | Name | Type |
| 1 | msdevspocpiappservice | App Service Plan |
| 2 | msdevspocpihighconsumptionappservice | App Service Plan |
| 3 | msdevspocpichangeprocessor | Function app |
| 4 | msdevspocpichangeprocessorapp | App service |
| 5 | msdevspocpinotificationreceiver | Function app |
| 6 | msdevspocpipopulatetracking | Function app |
| 7 | msdevspocpiwebhooksmanagerapp | App service |
| 8 | msdevspocpiappinsight | Application Insights |
| 9 | msdevspocpirediscache | Azure Redis Cache |
| 10 | msdevspocpikeyvault | Key Vault |
| 11 | msdevspocpisearch | Search Service |
| 12 | msdevspocpiservicebus | Service Bus Namespace |
| 13 | msdevspocpiwebhooks | Storage Account |
| 14 | msdevspocpidoctrack | Storage Account |

1. Webhooks Storage Account changes
   1. Following tables should have been created
      1. Configuration
      2. Subscriptions
   2. Configuration table should have 29 entries.
   3. In case of first-time deployment, please add/update below configuration items in the table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PartitionKey** | **RowKey** | **ConfigKey** | **ConfigValue** | **Restricted** |
| SPOCPI | HTMLInputValidation | HTMLInputValidation | <("[^"]\*"|'[^']\*'|[^'">])\*> | False |
| SPOCPI | AppInsightsInstrumentationKey | AppInsightsInstrumentationKey | Get the Instrumentation key for application insight | False |

1. DocTrack Storage Account changes
   1. Following tables should have been created
      1. DriveDelta
      2. DocumentTracking
      3. NotificationStorage
2. The below WebJobs are deployed to Webhooks app service and are in running state
   1. WebHooksManagerWebJob
3. The below WebJobs are deployed to Change processor app service and are in running state
   1. ChangeProcessorWebJob
4. KeyVault changes
   1. Below secrets should have been created
      1. AADAppClientId
      2. AADAppClientSecret
      3. RedisConnectionString
      4. SearchUpdateKey
      5. ServiceBusConnectionString
      6. DocTrackStoreConnectionString
      7. WebHooksStoreConnectionString
   2. Below app services should have been added under Access Policies and they should have Get permissions on secrets
      1. spocpichangeprocessor
      2. spocpichangeprocessorapp
      3. spocpinotificationreceiver
      4. spocpipopulatetracking
      5. spocpiwebhooksmanagerapp
      6. spocpiwebhooksmanagerapp
5. Search service changes
   1. Below indexes should have been created
      1. subscriptionstable-index
      2. documenttrackingtable-index
   2. Below indexers should have been created and their status is not Failed
      1. subscriptions-indexer
      2. documenttrackingtable-indexer
   3. Below data sources should have been created
      1. subscriptionstable
      2. documenttrackingtable
6. For each app service listed in services.csv file, find the corresponding appsettings json file in app settings folder and check if those app settings are copied to the app service.

# Maintenance activities

1. Keyvault secrets expiration date
   1. Monitor the keyvault secrets and renew the expired one’s regularly.
2. Renew the AAD App Client secret before expiration time. Raise a ticket in SNOW with MAHS team

# Miscellaneous

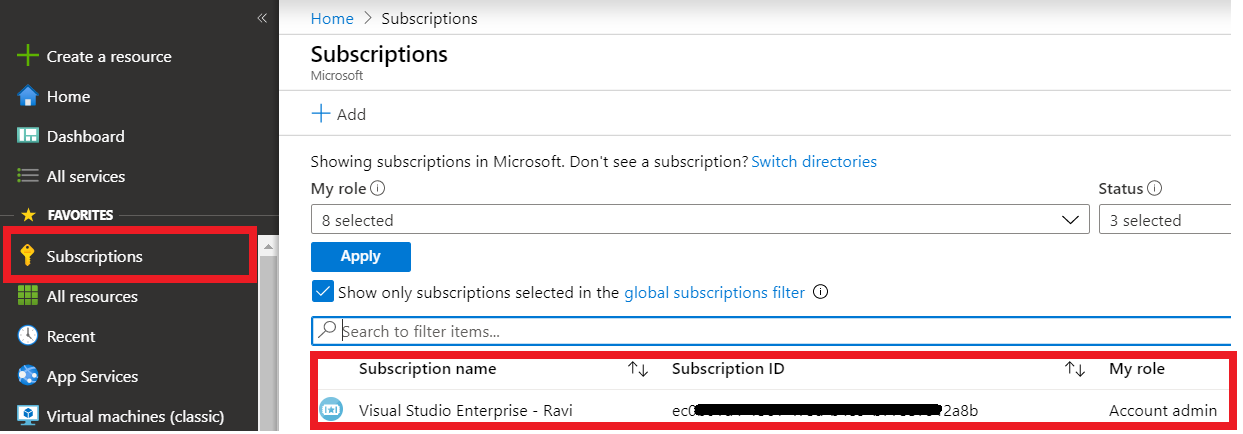


## Create AAD Application

1. Azure Subscription with minimum contributor level of access.
   1. To verify Go to [Azure Portal](http://portal.azure.com/) and login with azure credentials.

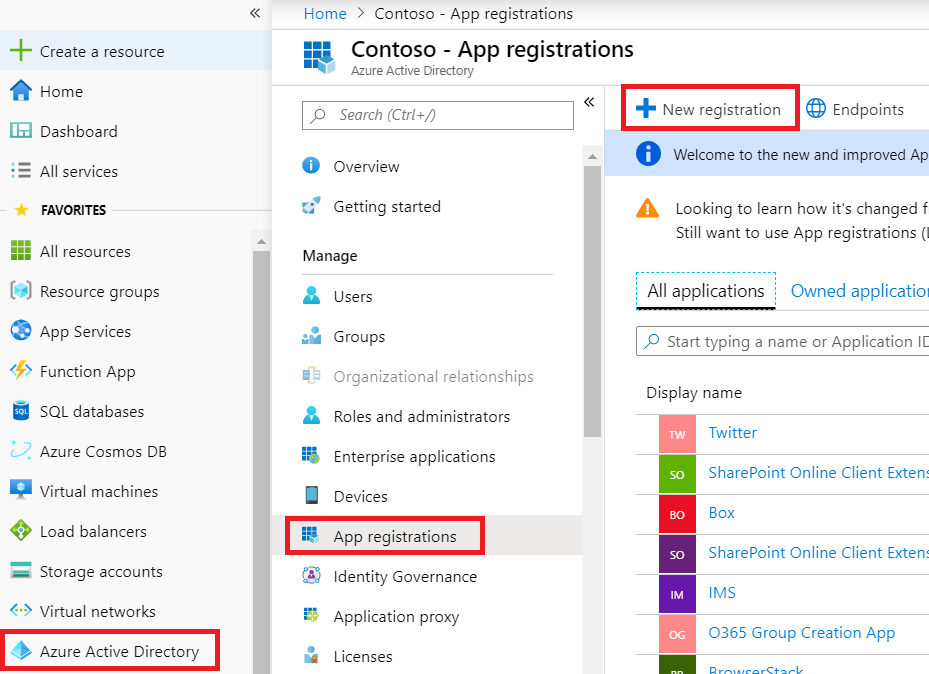
**Note:** Azure Portal user Experience may vary time to time, below screens are just for reference purpose.

* 1. If your account has access to more than one tenant, select your account in the top right corner, and set your portal session to tenant where you want to deploy the SPOCPI.
  2. Go to Portal Menu > subscriptions



* 1. Check My Role in the Subscriptions Table View.
  2. If the subscription is not displayed, **uncheck** **“Show only subscriptions selected in the global subscriptions filter”**

1. Azure AAD app registration with directory and sites read access.
   1. From Portal Menu select “Azure Active Directory”. Under manage select “App registrations” and click on “New registration”.

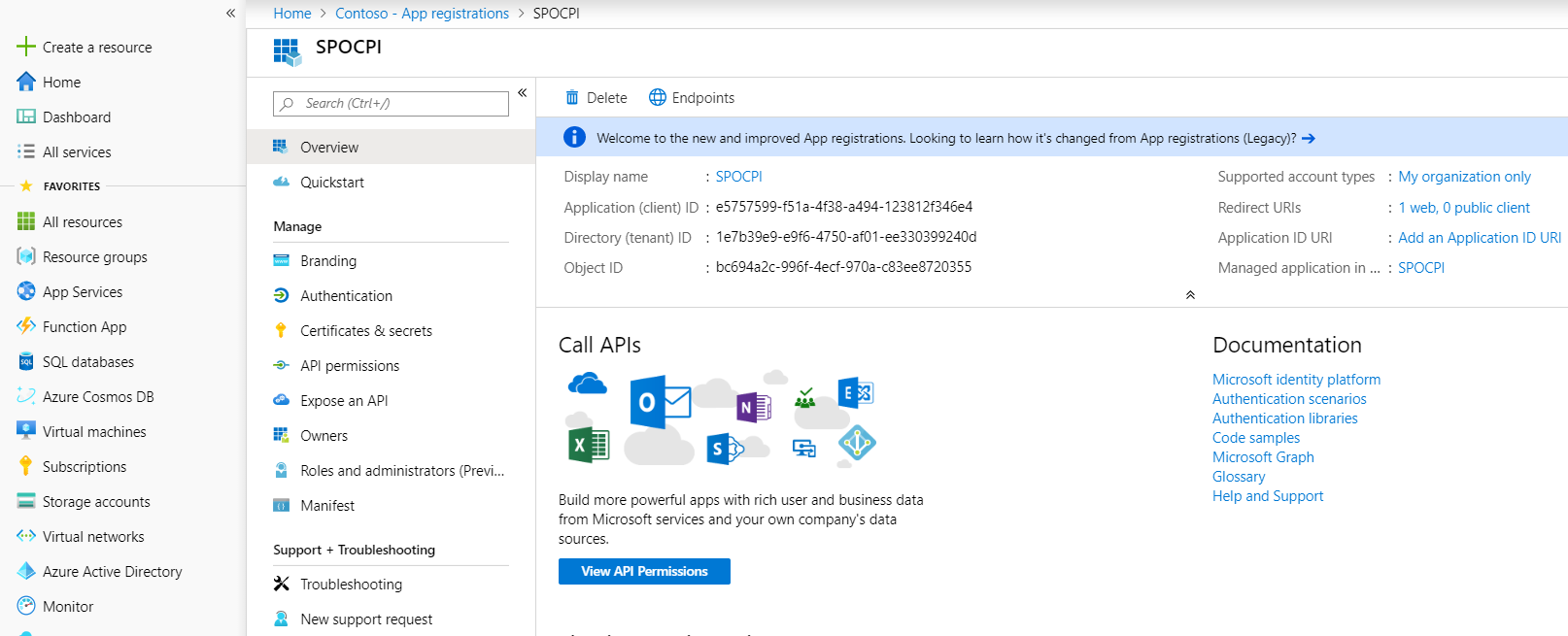


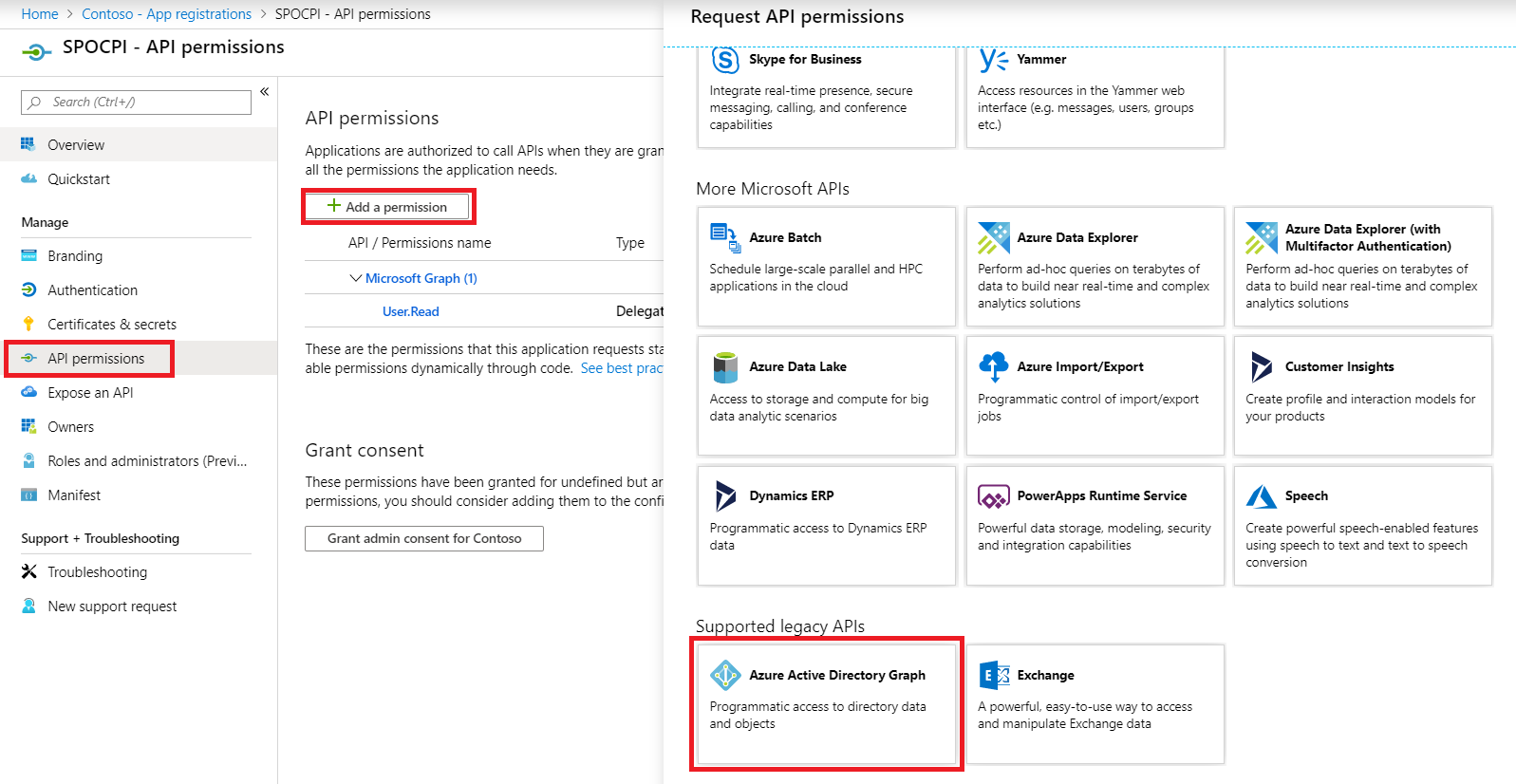
* 1. In **Register an application** page, fill the app registration Information.
     1. **Name:** Enter Application name that will be displayed to users of the app. ex :- SPOCPI.
     2. **Supported account types:** Select **Accounts in this organizational directory only.**
     3. **Redirect URI:** Select the type of app you're building, (Select **Web from the left dropdown**), and then enter the redirect URI (or reply URL) for your application followed by “/signin-odc”. Users would use this URL to sign into a web client application.  
        (ex:- <https://spocpiwebhooksmanagerapp.azurewebsites.net/signin-oidc>)
     4. Click on **Register.**

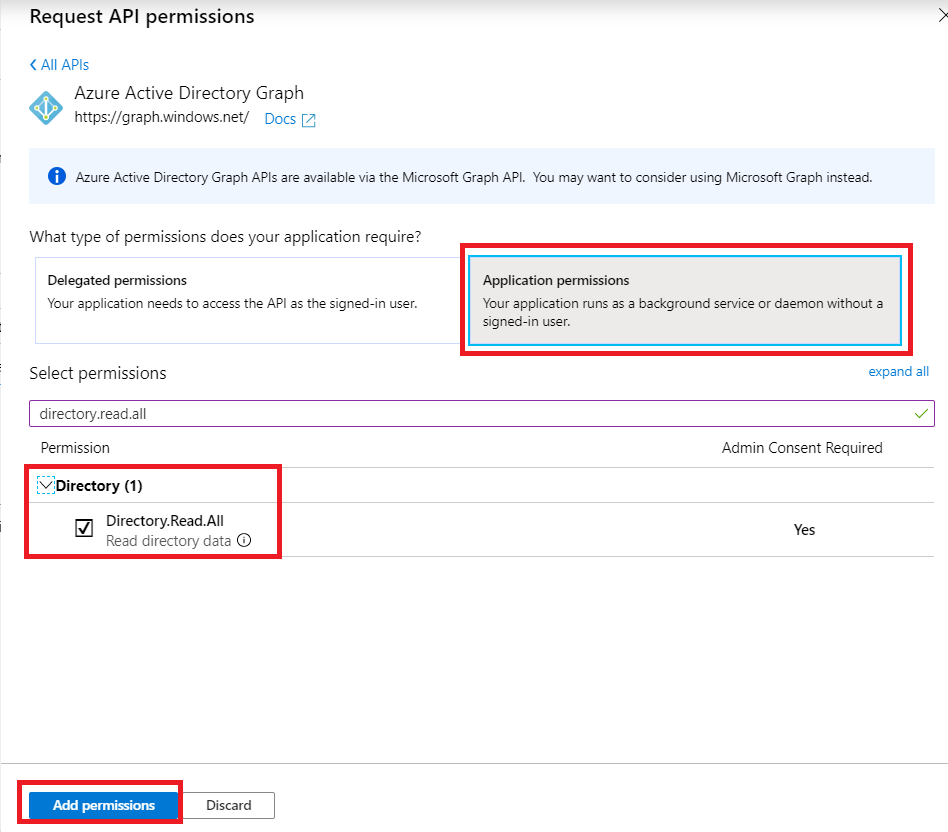
A screenshot of a social media post

Description automatically generated

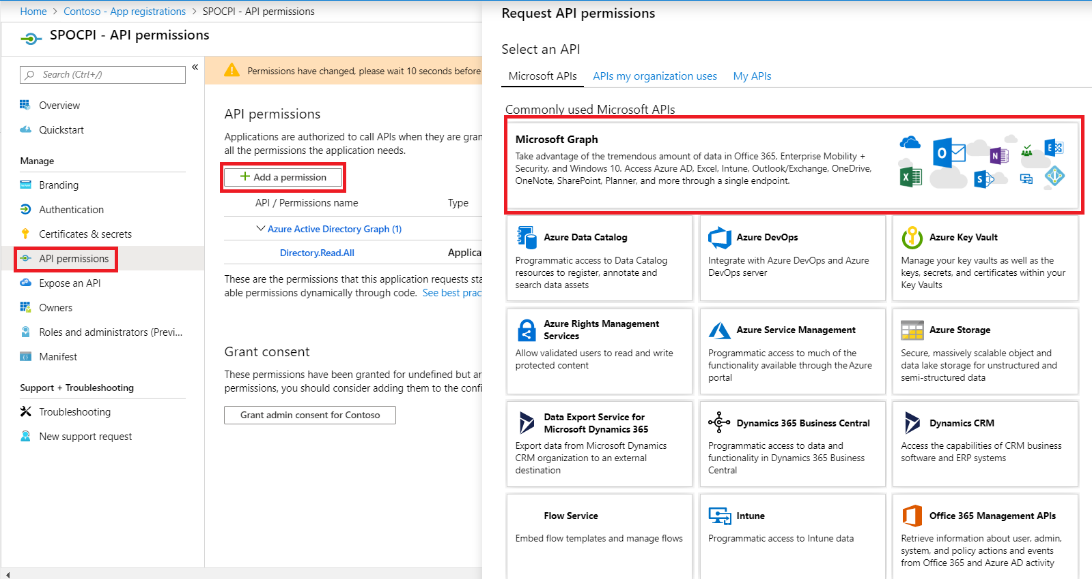
* + 1. Upon Successful registration Application Overview page gets displayed.



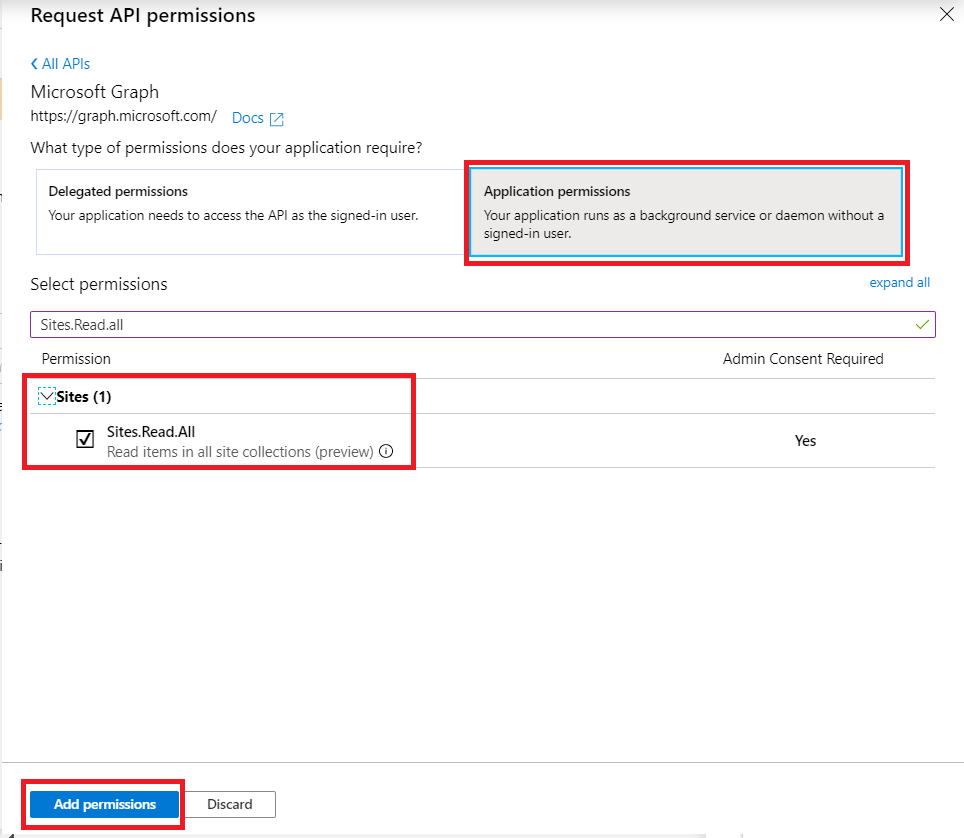
* + 1. AAD App needs **Azure Active Directory Graph** and **Microsoft Graph** Application permissions.
    2. To add Azure Active Directory Graph **(Directory.Read.All)** permissionfollow the below steps
    3. Under **Manage** select “**API Permissions**” then click on Add permissions and scroll down to the bottom. From Supported legacy APIs, select Azure Active Directory Graph.
    4. In Request API permission panel select “**Application permissions**” and check “**Directory.Read.All**” then click on “**Add permissions**”.



* + 1. Azure Active Directory permission gets added to the application.
    2. To add Microsoft Graph **(Sites.Read.All)** permission follow the below steps
    3. Under **Manage** select “**API Permissions**” then click “**Add a permission**”. Select “**Microsoft Graph”**.



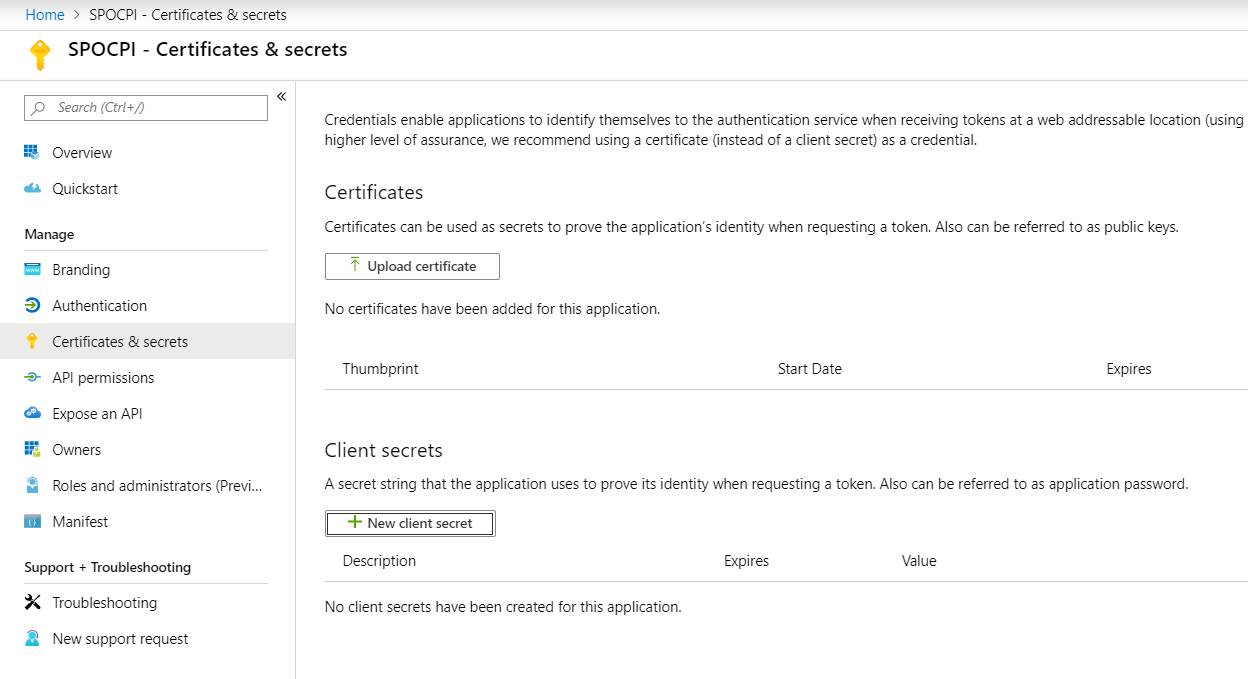
* + 1. In Request API permission panel select “**Application permissions**” and check “**Sites.Read.All**” then click on “**Add permissions**”.



* + 1. Microsoft Graph **“Sites.Read.All”** App permission gets added to the application.
    2. In API permissions panel get the permissions **Grant admin consent**.

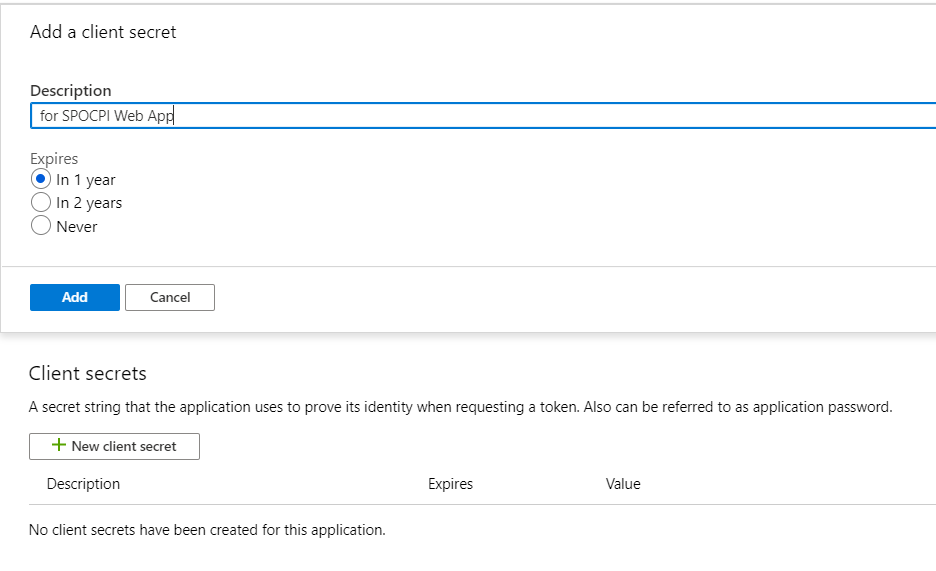
**Note :** If you have no access, get the consent from the Administrator

* + 1. Under Manage select “Certificates & secrets” and click on “New client secret”



* + 1. Add a description, select expiry, and click **Add**.

**Note:** For expiring secrets, refresh [Update AAD App Secrets](#_Update_AAD_App) for how to update secrets.



* + 1. A new secret will be added. **Copy the secret value and store it. It is needed for configuring Deployment.**

**Note:** Password won’t be displayed in plaintext later. So, make sure you copy it as and when added a secret