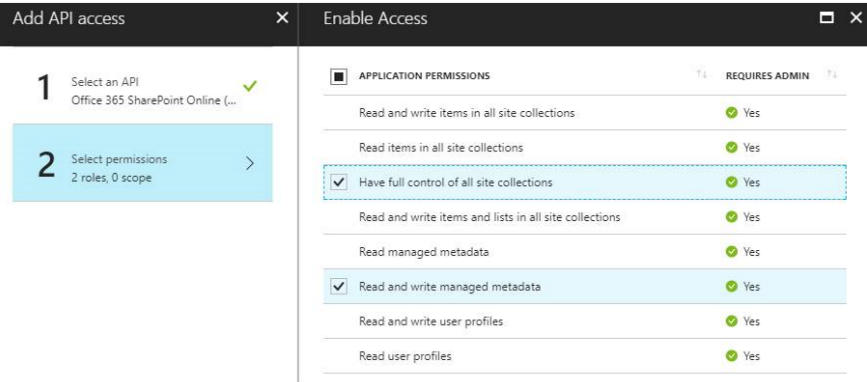
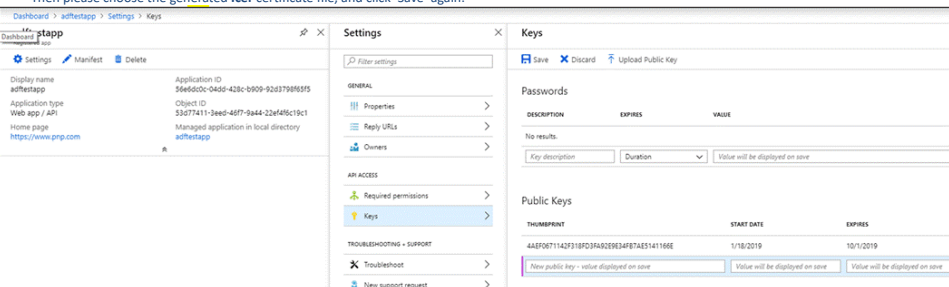
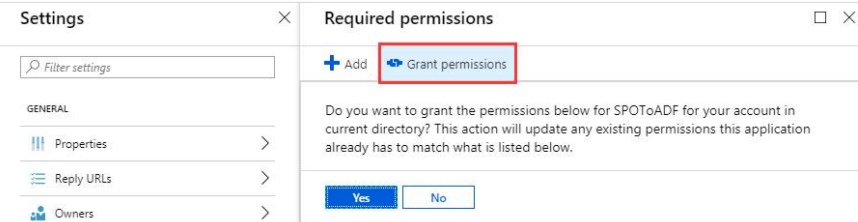


[OData] How to connect to SharePoint List Using OData Connector

Last updated by | Veena Pachauri | Mar 8, 2023 at 11:23 PM PST

Public doc is available:
<https://docs.microsoft.com/en-us/azure/data-factory/connector-sharepoint-online-list>

	201047- [OData] How to connect to SharePoint List Using OData Connector			
			ASC Onboard	
	Friday, January 25, 2019 1:17 PM			

SME	()
Symptoms	Customer wants to connect to Sharepoint online with Service Principal authentication
Cause	This is by design that there is no interactive OAuth supported with ADF V2
Resolution	<p>We need to use "AAD Service principal with Cert" auth type in OData to connect to SharePoint Online. First need follow this document to register the AAD service principal for SPO: https://docs.microsoft.com/en-us/sharepoint/dev/solution-guidance/security-apponly-azuread</p> <ol style="list-style-type: none"> create the self-signed X.509 Certificate using Create-SelfSignedCertificate.ps1 in above doc You will be asked to give a password to encrypt your private key, and both the .PFX file and .CER file will be exported to the current folder. registering an Azure AD application in the Azure Active Directory tenant that is linked to your Office 365 tenant select the option "Web app / API", and fill in the "Sign-on URL" with a URL (does not have to exist, e.g. https://www.pnp.com). click on "Required Permissions", and click on the "Add" button, a new blade will appear. You need to configure the following permissions: Office 365 SharePoint Online (Application Permission) <ul style="list-style-type: none"> Read and write managed metadata Have full control of all site collection  <ol style="list-style-type: none"> Upload the .cer file generated in Step 1 to AAD app go to the AAD app, "Settings" "Keys", "Upload Public Key". You could delete existing public keys, and 'Save' first. Then please choose the generated .cer certificate file, and click 'Save' again.  <ol style="list-style-type: none"> Consent your AAD app by clicking "Grant permissions" a. if you are tenant admin:  <ol style="list-style-type: none"> Otherwise, create a consent URL like the following: <a href="https://login.microsoftonline.com/<tenant>/adminconsent?client_id=<application id>&state=<something>">https://login.microsoftonline.com/<tenant>/adminconsent?client_id=<application id>&state=<something> Then ask your tenant admin to consent:

BertOnlineAzureADAppOnlyDemo
App publisher website: bertonline.onmicrosoft.com

BertOnlineAzureADAppOnlyDemo needs permission to:

- Have full control of all site collections
- Read and write managed metadata
- Sign in and read user profile

You're signed in as: bert.jansen@bertonline.onmicrosoft.com (admin)

If you agree, this app will be granted the specified application permission(s) to resources belonging to all users in your organization, and delegated permission(s) to resources belonging to the signed-in user. [More details](#)

Accept

Cancel

After above 5 steps, the action on AAD service principal is completed. Now we could return back to ADF OData connector.

1. Go back to Azure Data Factory, create a OData Linked Service, you need to upload the cert in .pfx format.
- Other config details:
- Service URL: this is the Sharepoint Online Site URL. It should be something like https://xxxxxxx.sharepoint.com/_vti_bin/listdata.svc/ if it does not contain any sub site, or https://xxxxxxxxx.sharepoint.com/sites/site2/_vti_bin/listdata.svc/ if it contains multi sub sites.
 - AAD resource: <https://xxxxxx.sharepoint.com/>
 - Tenant: the directory id where you registered the AAD app
 - Service Principal ID: AAD app ID

Edit Linked Service (OData)

Service URL *

https://.sharepoint.com/_vti_bin/listdata.svc/

Authentication type *

AAD Service principal with Cert

Please make sure your Selfhosted integration runtime is higher than version 3.12 if connecting via Selfhosted integration runtime.

AAD resource *

https://mswxos.sharepoint.com/

Tenant *

Service principal ID *

Service principal embedded cert

Azure Key Vault

Service principal embedded cert *

Choose File

No file chosen

Embedded cert password

Azure Key Vault

Embedded cert password

Annotations

Connection successful

Cancel

Test connection

Finish

Created with Microsoft OneNote 2016.

How good have you found this content?

