


[Rest Project Online] Connect to Project Online in an automated manner

Last updated by | Graziani Orcai | Mar 10, 2022 at 2:34 AM PST

Connect to Project Online in an automated manner

Issue

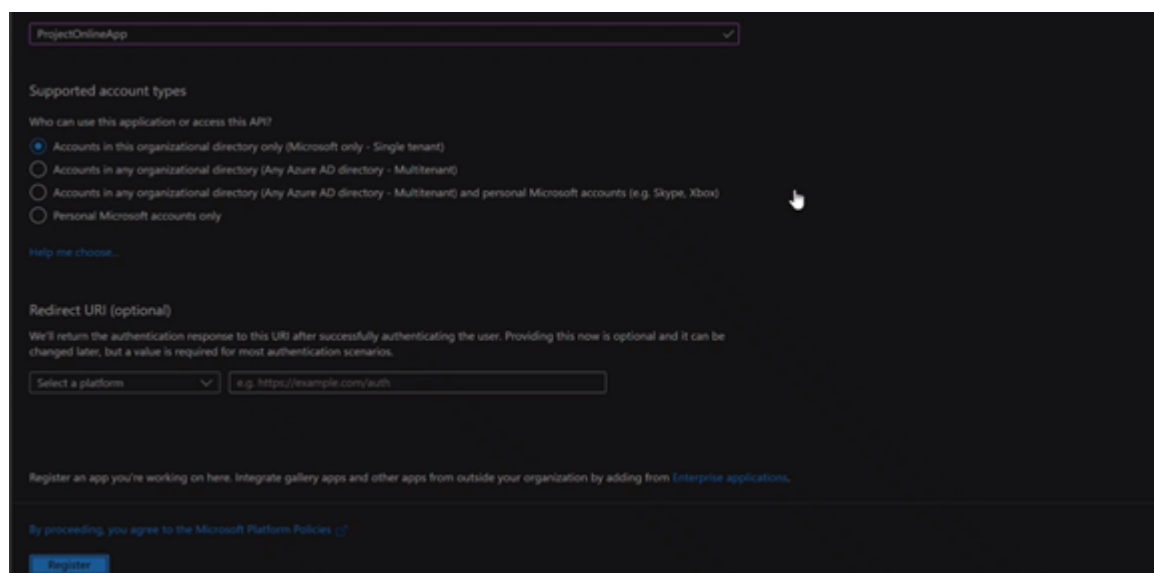
Even though we already have documented a possibility on how to connect to Project Online: [Copy data from OData sources - Azure Data Factory & Azure Synapse | Microsoft Docs](#) , this solution propose to generate the access token with another tool (eg. Postman) and use afterwards the access token to connect to Project Online from ADF. However, this solution is not the best one since the token will expire and customer needs to manually generate a new token and replace it back into ADF. Moreover, the normal authentication was not possible either due to the fact that Project Online requires user-based OAuth, which is not supported by ADF.

Solution

Having the above scenario and customer requirement, we have also worked with AAD team and also with Project Online team and have also found an alternative solution which will work automatically for customer. The solution will have at least 1 web activity to generate the access token and a second activity to use the access token to make the connection.

Prerequisites:

1. ADF account
2. App registration for Project Online with the following settings enabled:
 - a. Create a new app reg:



The screenshot shows the Microsoft App Registration portal. At the top, the application name 'ProjectOnlineApp' is entered in a dropdown menu. Below this, the 'Supported account types' section is visible, with the first option 'Accounts in this organizational directory only (Microsoft only - Single tenant)' selected. The 'Who can use this application or access this API?' section is also visible, with the same option selected. The 'Redirect URI (optional)' section is visible, with a text input field containing 'e.g. https://example.com/auth'. At the bottom, there is a 'Register' button.

- b. Configure permissions:

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Contoso

| API / Permissions name | Type | Description | Admin consent requ... | Status |
|-----------------------------|-----------|---|-----------------------|---------------------------|
| Microsoft Graph (1) | | | | *** |
| User.Read | Delegated | Sign in and read user profile | No | ✓ Granted for Contoso *** |
| SharePoint (1) | | | | *** |
| ProjectWebAppReporting.Read | Delegated | Read ProjectWebApp OData reporting data | No | ✓ Granted for Contoso *** |

To view and manage permissions and user consent, try [Enterprise applications](#).

c. Add a secret to the app:

ProjectOnlineApp | Certificates & secrets

Search (Ctrl+F) Got feedback?

Overview Quickstart Integration assistant

Manage

Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators | Preview Manifest Support + Troubleshooting Troubleshooting New support request

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

| Description | Expires | Value | Copy to clipboard | Alt ID |
|-------------|-----------|---------------------------------|--------------------------------------|--------|
| ADF | 1/14/2023 | G5TQ-E2VZJwC00wQvDrZpXg19w5d... | 55ecb390-eb16-49b6-bd83-c41f8dbc3b80 | |

d. Collect the endpoint as per below, to be used further:

Search (Ctrl+F) Delete Endpoints Preview features

Overview Quickstart Integration assistant

Manage

Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators | Preview Manifest Support + Troubleshooting Troubleshooting New support request

Endpoints

Display name

Application (client) ID : 36420932-6a39-48d2-9f6d-77560d81e18

Object ID : 2e158468-4b4b-4a21-a4d8-1a8b059e11e

Directory (tenant) ID : 729885f-8691-41af-91ab-2d7cd011b647

Supported account types : [My organization only](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory. Applications will need to be upgraded to Microsoft Entra ID.

Get Started Documentation

Build your app

The Microsoft identity platform is an authentic based authentication solution.

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own.

OAuth 2.0 authorization endpoint (v2) <https://login.microsoftonline.com/729885f-8691-41af-91ab-2d7cd011b647/oauth2/authorize>

OAuth 2.0 token endpoint (v2) <https://login.microsoftonline.com/729885f-8691-41af-91ab-2d7cd011b647/oauth2/token>

OAuth 2.0 authorization endpoint (v1) <https://login.microsoftonline.com/729885f-8691-41af-91ab-2d7cd011b647/oauth2/authorize>

OAuth 2.0 token endpoint (v1) <https://login.microsoftonline.com/729885f-8691-41af-91ab-2d7cd011b647/oauth2/token>

OpenID Connect metadata document <https://login.microsoftonline.com/729885f-8691-41af-91ab-2d7cd011b647/v2.0/.well-known/openid-configuration>

Microsoft Graph API endpoint <https://graph.microsoft.com>

Federation metadata document <https://login.microsoftonline.com/729885f-8691-41af-91ab-2d7cd011b647/federationmetadata/2007-06/federationmetadata.xml>

WS-Federation sign-on endpoint <https://login.microsoftonline.com/729885f-8691-41af-91ab-2d7cd011b647/wsfed>

SAML, P sign-on endpoint <https://login.microsoftonline.com/729885f-8691-41af-91ab-2d7cd011b647/saml2>

SAML, P sign-out endpoint <https://login.microsoftonline.com/729885f-8691-41af-91ab-2d7cd011b647/saml2>

e. Also keep the client id and client secret in mind from app registration overview.

- Azure cloud-only account.** These accounts can go directly to the login.microsoftonline.com /token endpoint to request a token from Azure. After the creation of a cloud-only account, it has to be given permissions to Project Online and then used in the Postman ROPC flow to see if you successfully receive a

token without further steps to be applied in Postman for token generation. Moreover, when you log into Project Online with this account, you need to be able to access the resource you want to retrieve data from.

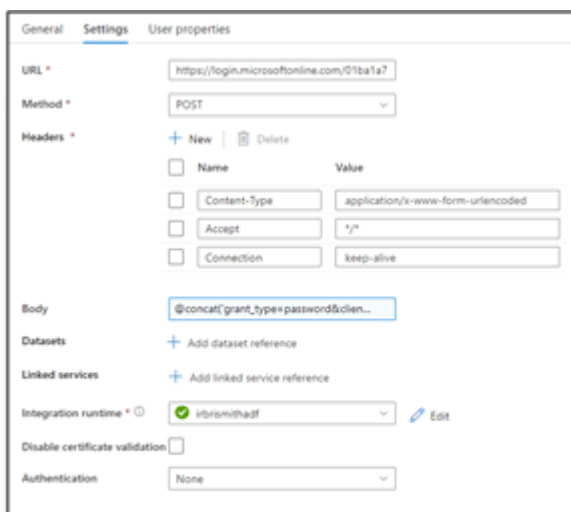
Please consider that ROPC OAuth flow is not supported with ADFS accounts (federated accounts) because the token provider for these accounts is not Azure, but your local ADFS server.

After the prerequisites are done, we can continue with ADF configuration:

1. Configure web activity to retrieve the token:



Web activity on ADF:

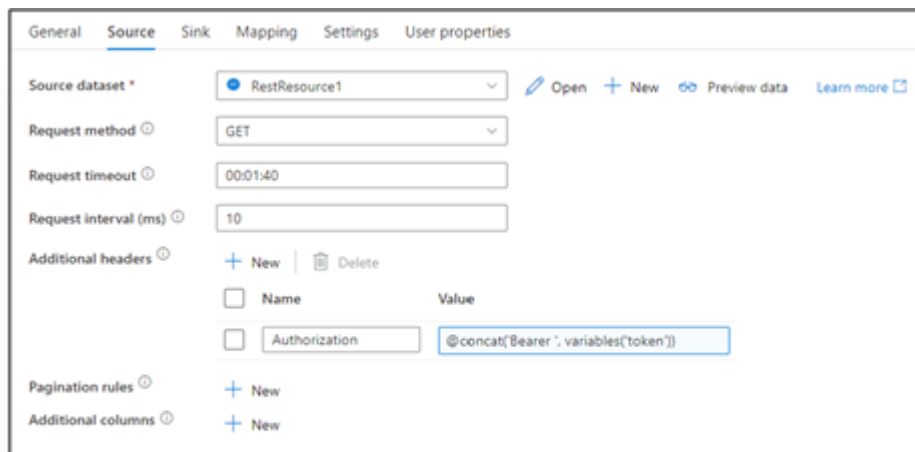




2. Create a copy activity where the source will be the connection to Project Online using the token generated and move the data to the sink:


```
{
  "name": "Read OData and save to Blob",
  "type": "Copy",
  "dependencies": [
    {
      "activity": "GetToken",
      "dependencyConditions": [
        "Succeeded"
      ]
    }
  ],
  "policy": {
    "timeout": "7.00:00:00",
    "retry": 0,
    "retryIntervalInSeconds": 30,
    "secureOutput": false,
    "secureInput": true
  },
  "userProperties": {},
  "typeProperties": {
    "source": {
      "type": "RestSource",
      "url": "https://api.projectonline.com/odata/...",
      "requestTimeout": "00:05:00",
      "requestInterval": "00:00:00.010",
      "requestMethod": "GET",
      "additionalHeaders": {
        "Authorization": {
          "value": "@concat('bearer ', variables('token'))",
          "type": "Expression"
        }
      },
      "paginationRules": {
        "supportRPCSMB": true
      }
    },
    "sink": {
      "type": "JdbcSink",
      "storeSettings": {
        "type": "AzureBlobStorageWriteSettings",
        "copyBehavior": "MergeFiles"
      },
      "formatSettings": {
        "type": "JsonFormatSettings"
      }
    },
    "enableStaging": false
  },
  "inputs": [
    {
      "referenceName": "RestResources",
      "type": "DatasetReference"
    }
  ],
  "outputs": [
    {
      "referenceName": "Jdbc",
      "type": "DatasetReference"
    }
  ]
}
```

Copy activity source configuration on ADF:



The screenshot shows the 'Source' tab of the REST connector configuration in Azure Data Factory. The 'Source dataset' is set to 'RestResource1'. The 'Request method' is 'GET'. The 'Request timeout' is '00:01:40'. The 'Request interval (ms)' is '10'. Under 'Additional headers', there is a table with one row: 'Authorization' with the value '@concat("Bearer ", variables("token"))'. There are also buttons for 'New', 'Delete', 'Open', 'Preview data', and 'Learn more'.

| Name | Value |
|---------------|--|
| Authorization | @concat("Bearer ", variables("token")) |

Original internal work from Project Online can also be found here: [GitHub - LunchWithaLens/adf: Repo for Azure Data Factory stuff](#) 

How good have you found this content?



-