PowerBi Embedded walkthrough

There are two scenarios which will allow us to not authenticate the user, App owns data and Service Principal. Both require an Azure AD app registration:

Info:

MAIN EMBEDDING METHODS:

===========================================================================

APP OWNS DATA:  "For your customers". Essentially, all PowerBI Resources are accessed through a "Master Account", which makes all the API calls. Therefore, all permissions for PowerBI content use the permissions applied to the Master account.

<https://docs.microsoft.com/en-us/power-bi/developer/embed-sample-for-customers>

USER OWNS DATA: "For your organization". All users authenticate to PowerBI. This is essentially an extension of the PowerBI Service. Therefore, permissions at the account level are applied to the user accessing PowerBI resources through the Embedded solution that has been built.

<https://docs.microsoft.com/en-us/power-bi/developer/embed-sample-for-your-organization>

SERVICE PRINCIPAL: "App-Only authentication" - Essentially you are not authenticating as a user, but the AAD app registration itself. This method is ideal for automation of PowerBI administration programmatically.

<https://docs.microsoft.com/en-us/power-bi/developer/embed-service-principal>

MINOR EMBEDDING METHODS - NO CONFIG REQUIRED:

==============================================================================

PUBLISH TO WEB: you are essentially given an HTML tag that will display the requested resource. There is no authentication and security applied to this, so it is generally discouraged to use this option. You can easily insert the HTML tag into any web page.

<https://docs.microsoft.com/en-us/power-bi/service-publish-to-web>

SECURE EMBED: Similar to Publish to web, you are given an HTML tag to include in a web page. This Tag requires you to authenticate to PowerBI so there is security built in. All PowerBI Permissions are applied based on the user sign in, so you must have access in the PowerBI service to see the embedded content.

<https://docs.microsoft.com/en-us/power-bi/service-embed-secure>

EMBED IN SHAREPOINT:

This option takes the Authentication token from SharePoint and passes into PowerBI, so you are not prompted to authenticate again. Since Auth is being passed, this is still a secure option.

<https://docs.microsoft.com/en-us/power-bi/service-embed-report-spo>

**STEP 1: SET UP AAD APP REGISTRATION**

Go ahead and login to the azure portal: <https://portal.azure.com/#home>  .

Click on "Azure active directory" on the left hand side.

Machine generated alternative text:
All resources 
CO) Resource groups 
App 
Services 
SQL databases 
Azure Cosmos DB 
Virtual machines 
Load balancers 
Storage accounts 
Virtual networks 
Azure Active Directory 

Go ahead and select "App registrations"

Machine generated alternative text:
Users 
Groups 
Organizational relationshib 
Roles and administrators 
Enterprise applications 
Devices 
App registrations 
Identity Governance 
Application proxy 

Click on "New Registration" , give it a name and press Register.

Machine generated alternative text:
* Name 
The user-facing display name for this application (this can be changed later). 
AADApp 
Supported account types 
Who can use this application or access this API? 
• Accounts in this organizational directory only (Contoso only - Single tenant) 
O 
Accounts in any organizational directory (Any Azure AD directory - Multitenant) 
O 
Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, XBox) 
Help me choose... 
Redirect URI (optional) 
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be 
changed later, but a value is required for most authentication scenarios. 
By proceeding, you agree to the Microsoft Platform Policies Z 
Register 

From Here, Copy paste your Application (Client) ID and Directory (Tenant) ID into a notepad. We will need these for our embedded labs.

Then go ahead and click "View API permissions"

Machine generated alternative text:
Delete Endpoints 
O 
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? 
Overview 
Quickstart 
Manage 
Branding 
Authentication 
Certificates & secrets 
API permissions 
O Expose an API 
15,', Owners 
Roles and administrators (Previ... 
Manifest 
Support + Troubleshooting 
Troubleshooting 
New support request 
Display name 
Application (client) ID 
Directory (tenant) ID 
Object ID 
Call APIs 
AA DAPP 
. bceaf21b 
: 6a2ab1f6 
: 21 cda90e 
S 
-985e-425e-a559-9374c9038743 
-9b9e-4a34-86e3-83952c51faff 
-4 a -48 
-9270-2578b0872b5c 
Supported account types 
Redirect URIS 
Managed application in . 
Documentation 
Microsoft identity platform 
Authentication scenarios 
Authentication libraries 
Code samples 
Microsoft Graph 
Glossary 
Help and Support 
My 
Ad c 
AAC 
Build more powerful apps with rich user and business data 
from Microsoft services and your own company's data 
sources. 
View API Permissions 
Sign in users in 5 minutes 

Go Ahead and click "Add a Permission", Then Select PowerBI Service.

Machine generated alternative text:
Select an API 
Microsoft APIs APIs my organization uses 
Commonly used Microsoft APIs 
Microsoft Graph 
My APIs 
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + 
Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, 
OneNote, SharePoint, Planner, and more through a single endpoint. 
Azure Data Catalog 
Programmatic access to Data Catalog 
resources to register, annotate and 
search data assets 
/A 
Azure Service Management 
Programmatic access to much of the 
functionality available through the Azure 
portal 
Programmatic access to Intune data 
Azure DevOps 
Integrate with Azure DevOps and Azure 
DevOps server 
Dynamics 365 Business Central 
Programmatic access to data and 
functionality in Dynamics 365 Business 
Central 
Office 365 Management APIs 
Retrieve information about user, admin, 
system, and policy actions and events 
from Office 365 and Azure AD activity 
Azure Rights Management 
Services 
Allow validated users to read and write 
protected content 
Flow Service 
Embed flow templates and manage flows 
Power Bl Service 
Programmatic access 
to Dashboard resources such 
as Datasets, Tables, and Rows in Power 81 

Select "Delegated Permissions".

For the scope of this lab, we will be Giving our API all permissions. Go ahead and select all API permissions for PowerBI, and press Add.

Scroll to the bottom of the page, and select "Grant Admin Consent"

Machine generated alternative text:
These are the permissions that this application requests statically. You may also request user consent- 
able permissions dynamically through code. See best practices for requesting permissions 
Grant consent 
As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all use 
users will not be shown a consent screen when using the application. 
Grant admin consent for Contoso 

Once that is done, Go ahead and Select "New Client Secret" and create your client secret. For expires, select "Never"

Copy paste the Client secret into the notepad. **( NOTE: CLIENT SECRET IS ONLY NEEDED FOR SERVICE PRINCIPAL )**

Machine generated alternative text:
Overview 
Quickstart 
Manage 
Branding 
Authentication 
Certificates & secrets 
API permissions 
O Expose an API 
Owners 
Roles and administrators (Previ... 
Manifest 
Support + Troubleshooting 
Troubleshooting 
New support request 
Certificates 
Certificates can be used as secrets to prove the application's identity when requesting a token. 
Upload certificate 
No certificates have been added for this application. 
THUMBPRINT 
Client secrets 
START DATE 
A secret string that the application uses to prove its identity when requesting a token. Also can 
+ New client secret 
DESCRIPTION 
No client secrets have been created for this application. 
EXPIRES 
VALUE 

We have now configured our AAD app registration, so that we can begin to Manipulate PowerBI Programmatically !

**STEP 2: GET AUTH TOKEN – pick either App-owns or Service Principal**

In order for us to make calls to the PowerBI REST API, we need to authenticate first. We do this by crafting an HTTP packet with specific information and sending the packet to a login endpoint.

POSTMAN is a tool specifically used for API development and it is what we will be using for this scenario. Download POSTMAN here: <https://www.getpostman.com/>

**APP-OWNS DATA ( GET AUTH TOKEN )**

Start POSTMAN, and in the top left, select New, and create a new collection. I named mine PowerBI Embedded.

Go ahead and press "Add Requests" . I named mine "Authentication".

Machine generated alternative text:
Q Filcer 
History 
Import 
Collections 
Runner 
PowerBl Embedded 
APIS 
Run 
Trash 
Documentation 
View in web 
+ New Collection 
Azure AD v2.O Protocols 
13 requests 
I request 
PowerBl Embedded 
O requests 
Monitors 
Mocks 
Change log 
Learn how to document your requests 
PowerBI Embedded 
This collection is empty. Add requests to this collection and 
create folders to organize them 
This collection is empty. Add requests to this 
collection and create folders to organize them 
To Share 
2 requests 

Click on your request and press "Open in Builder".

Your screen will now take you to the Packet building screen.

Machine generated alternative text:
GET Authentication 
Authentication 
Enter request URL 
Pre-request Script 
VALUE 
Value 
Tests 
No Environment 
Cookies 
Exa mples (O) 
Save 
Pa rams 
Authorization 
H eaders 
Body 
Code 
Query Pa rams 
Response 
Comments (O) 
auk Edit 
DESCRIPTION 
Description 

Go ahead and Select the Body tab, and x-www-form-urlencoded.

Machine generated alternative text:
GET Authentication 
Authentication 
Enter request URL 
Pa rams 
none 
Response 
Authorization 
form-data 
Headers (1) 
Body 
x-mmnpform-urlencoded 
Pre-request Script 
binary 
VALUE 
Value 
Tests 
BETA 
GraphQL 
DESCRIPTIO 
Descriptio 

From there, Enter the following in the Request URL box: <https://login.microsoftonline.com/common/oauth2/token>

And change the method to POST.

Machine generated alternative text:



Now, fill out the Key-Value Pairs using the client(application) ID

NOTE: please ignore the client secret in the screenshot, its not required for this scenario.

Grant type: Password

client\_id: <put client ID here>

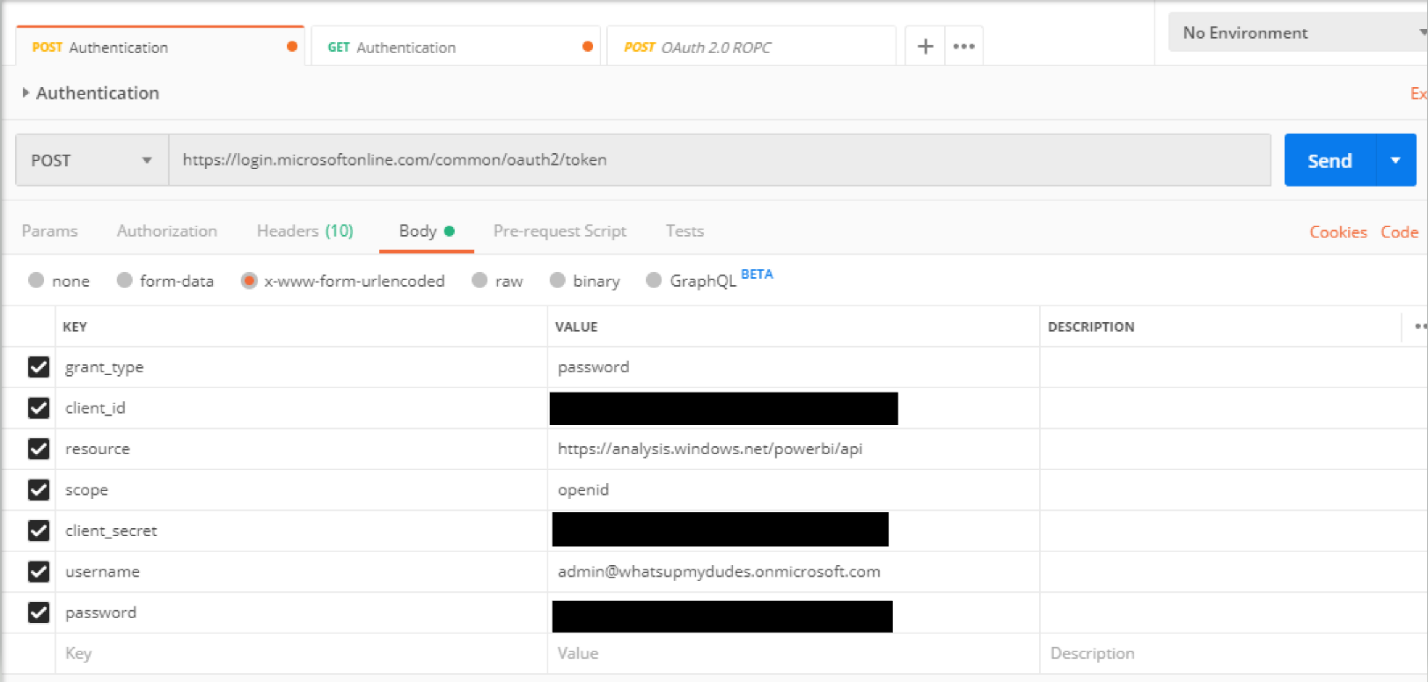
grant\_type:password

resource:https://analysis.windows.net/powerbi/api

scope: openid

username: < Your Email address>

password: <your account password>



Go Ahead and press "Send". You should see the token and a 200 HTTP status code.

Machine generated alternative text:



We have now successfully retrieved our Auth Token!

Go ahead and copy the Access\_token, and create a new request by pressing the + button on the tab.

Click on the "Authorization" tab, and Select OAuth2.0 as the auth type. Paste your access token into the corresponding box.

Machine generated alternative text:



You should get the JSON response with the Bearer token "access\_token" in the response.

Open a new tab, click on the "Authorization" option, and copy paste your access token:

Machine generated alternative text:



Enter the following URL into the request URL: <https://api.powerbi.com/v1.0/myorg/availableFeatures>,

And press Send.

Machine generated alternative text:



You should be returned the following with a 200 Status code.

Congrats! We have successfully authenticated and called the API. Using Access tokens, we can now call the specific API endpoints to manipulate the PowerBI service. This document houses all of the API endpoints and necessary permissions needed to call them:

<https://docs.microsoft.com/en-us/rest/api/power-bi/>

**SERVICE PRINCIPAL (GET AUTH TOKEN)**

Go ahead and navigate to the Azure Portal and Navigate to our App registration. We need to get the Object ID and copy it to our notebook. (This notebook should already have Tenant ID, Application ID, and Client secret in there).

Application (client) ID 
bceaf21b-985e-425e-a559-9374c9038743 
Directory (tenant) ID 
6a2ab1f6-4d4a48b4-9270-2578b0872b5c 
Object ID 
21 cda90e-9b9e-4a34-86e3-83952c51faff 

Once we have that, go back to the AAD page in the Azure Portal.

Go ahead and click on Groups, and select "new group"

Home > Contoso > Groups - All groups 
Groups - All groups 
Contoso - Azure Active Directory 
All groups 
Deleted groups 
Settings 
General 
Expiration 
Naming policy 
Activity 
Access reviews 
Audit logs 
Troubleshooting + Support 
Troubleshoot 
New support request 
+ New group Delete Refresh 
Columns 
Got 
NAME 
Embed.. 
SPNde... 
OBJECT ID 
f6a47c9c-f559... 
6c687e04-b5e... 
GROUP TYPE 
Office 
Security 
MEMBERSHIP TY 
Assigned 
Assigned 

Go ahead and Enter the Name of the security group, then add your AAD app registration to the security group:

Home > Contoso > Groups - All groups > New Group 
New Group 
* Group type 
Security 
* Group name O 
Serviceprincipal 
Group description O 
Enter a description for the group 
* Membership type 
o 
Assigned 
Owners 
Members 
Add members 
Select member or invite an external user O 
AADApp 
AADAPP 
Selected members: 
AA DAPP 

Now Navigate to the PowerBI web service, and login to our test tenant.

Once there, go to the admin portal (click on the settings icon in the top right) and click on "Tenant Settings". Scroll down to "Developer settings" and turn on "Allow Service Principals to use PowerBI API's".

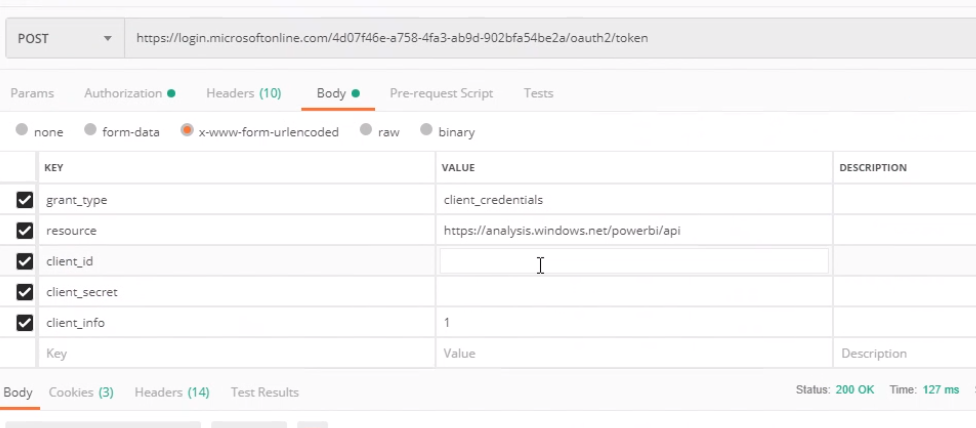
Admin portal 
Usage metrics 
Users 
Audit logs 
Tenant settings 
Capacity settings 
Embed Codes 
Organizational visuals 
Dataflow settings 
Workspaces 
Settings enabled for the entire organization apply to all users and service principals 
Disabled for the entire organization 
Developer settings 
Embed content in apps 
Enabled for the entire organization 
Allow service principals to use Power Bl APIs 
Enabled for a subset of the organization 
Web apps registered in Azure Active Directory (Azure AD) will use an assigned service 
principal to access Power Bl APIs without a signed in user. To allow an app to use service 
principal authentication its service principal must be included in an allowed security 
group. Learn more 
Enabled 
Service principals can use APIs to access tenant-level features controlled by Power 
Bl service admins and enabled for the entire organization or for security groups 
theVre included in. You can control access of service principals by creating 
dedicated security groups for them and using these groups in any Power Bl 
tenant level-settings. Learn more 

Add the security group we previously created to enable the Service Principal, and press apply.

Go ahead and pick a workspace v2 that we currently have, (or create one), and add the security group as an admin to that workspace.

Then Go ahead and open up PostMan, and format the call like the picture below.

NOTE: THE TENANT ID MUST BE INCLUDED IN THE URL FOR AUTH TOKEN CALL



Grant\_type client\_credentials

Resource <https://analysis.windows.net/powerbi/api>

Client\_id

Client\_secret

Client\_info 1