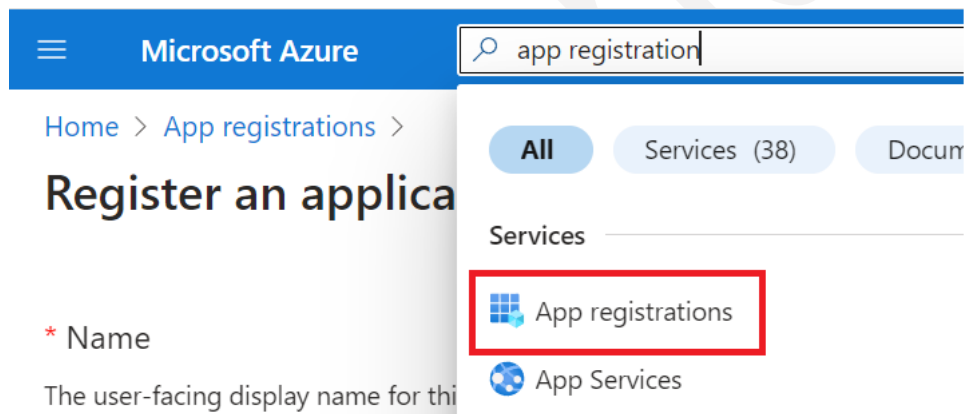


Set up Power BI REST API Tutorial

Go to app registrations in Azure

Create a new app



The screenshot shows the Microsoft Azure portal interface. At the top, there is a blue navigation bar with the text "Microsoft Azure" and a search bar containing the text "app registration". Below the navigation bar, the breadcrumb "Home > App registrations >" is visible. The main heading is "Register an applica". A search filter is applied, showing "All", "Services (38)", and "Docum". Under the "Services" section, two results are listed: "App registrations" (highlighted with a red box) and "App Services".

Microsoft Azure

Home > App registrations >

Register an applica

* Name

The user-facing display name for thi

app registration

All Services (38) Docum

Services

- App registrations
- App Services

Go to Certificates and secrets

Click on New client secret

Microsoft Azure Search resources, services, and docs (G+)

Home > App registrations > App Power BI REST API

App Power BI REST API | Certificates & secrets

Search

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets**
 - Token configuration
 - API permissions
 - Expose an API
 - App roles

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication scheme). For a higher level of assurance, we recommend using a certificate (instance).

Application registration certificates, secrets and federated credentials can be found here.

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

A secret string that the application uses to prove its identity when requesting tokens.

+ New client secret

Description	Expires	Value
No client secrets have been created for this application.		

Copy the value of the secret right after creation

Save it somewhere safe

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	secret ID
SecretPowerBIRESTAPI	3/6/2025	[REDACTED]	Copied [icon]

Copy the Application (client) ID

Copy the Directory (tenant) ID

[Home](#) > [App registrations](#) >

 **App Power BI REST API**  ...

 Delete  Endpoints  Preview features

 Overview

 Quickstart

 Integration assistant

 Diagnose and solve problems

▼ Manage

 Branding & properties

 Authentication

 Certificates & secrets

 Token configuration

^ Essentials

Display name

[App Power BI REST API](#)

Application (client) ID

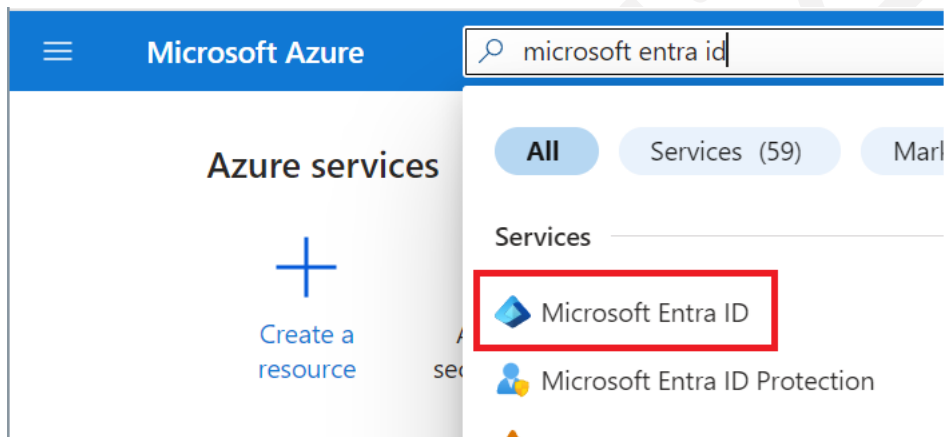
Object ID

Directory (tenant) ID

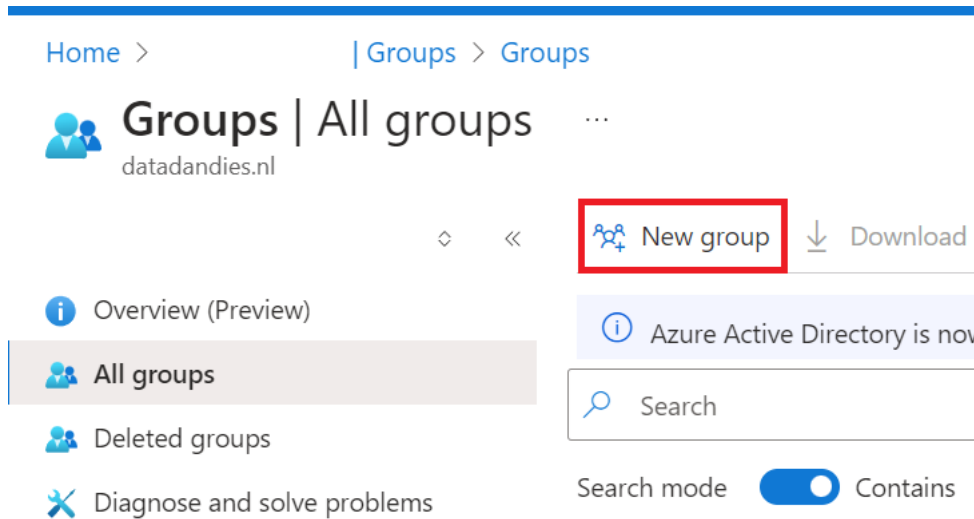
Supported account types

[My organization only](#)

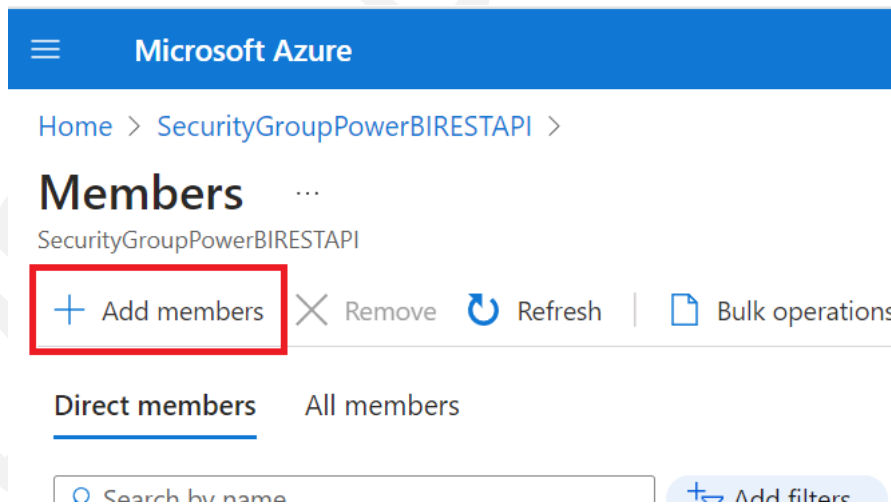
Go to Microsoft Entra ID



Create a new security group



Add the app that you created earlier to the newly minted security group as a member



Generate a Bearer Token

With Postman it can be done like this:

Enter the Application (client) ID as a collection-level variable

Enter the Directory (tenant) ID as a collection level variable

Enter the secret as a collection level variable

Overview Authorization • Scripts Tests Variables • Runs

These variables are specific to this collection and its requests. Learn more about [collection variables](#)

Filter variables

	Variable	Initial value	Current value
<input checked="" type="checkbox"/>	tenant_id		
<input checked="" type="checkbox"/>	client_secret		
<input checked="" type="checkbox"/>	client_id		

Do a POST API call using the following URL:

https://login.microsoftonline.com/{{tenant_id}}/oauth2/v2.0/token

Do not enter any params and use no authorization

Use the following Headers

POST ▼ | https://login.microsoftonline.com/{{tenant_id}}/oauth2/v2.0/token

Params Authorization Headers (9) Body ● Scripts Tests Settings

Headers 🔍 Hide auto-generated headers

Key	Value
<input checked="" type="checkbox"/> Cookie	fpc=Ap6giHqUf0JlsMJz-jNs7Eq2SqmpAQAAABffbd4OAAAA; stsservicecookie=estsfd; x-ms-gateway-slice=estsfd
<input checked="" type="checkbox"/> Postman-Token	<calculated when request is sent>
<input checked="" type="checkbox"/> Content-Type	application/x-www-form-urlencoded
<input checked="" type="checkbox"/> Content-Length	<calculated when request is sent>
<input checked="" type="checkbox"/> Host	<calculated when request is sent>
<input checked="" type="checkbox"/> User-Agent	PostmanRuntime/7.41.2
<input checked="" type="checkbox"/> Accept	*/*
<input checked="" type="checkbox"/> Accept-Encoding	gzip, deflate, br
<input checked="" type="checkbox"/> Connection	keep-alive

Use the following body

POST ▼ | https://login.microsoftonline.com/{{tenant_id}}/oauth2/v2.0/token

Params Authorization Headers (9) Body ● Scripts Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL

Key	Value
<input checked="" type="checkbox"/> grant_type	client_credentials
<input checked="" type="checkbox"/> client_id	{{client_id}}
<input checked="" type="checkbox"/> client_secret	{{client_secret}}
<input checked="" type="checkbox"/> scope	https://analysis.windows.net/powerbi/api/.default

The response will be your Bearer Token that you set as a variable at the collection level, just like e.g. the Application (client) ID

```
Body Cookies (3) Headers (15) Test Results Status: 200 OK Time: 169 ms Size: 2.02 KB Save as example
Pretty Raw Preview Visualize JSON
1 {
2   "token_type": "Bearer",
3   "expires_in": 3599,
4   "ext_expires_in": 3599,
5   "access_token":
6 }
```

Go to the Power BI Service and click on the admin portal

Add the security group that you created in Azure Entra ID in order to ensure that the app that you registered can use service principals instead of credentials to authenticate to Fabric APIs

Admin portal

Tenant settings

Usage metrics

Users

Premium Per User

Audit logs

Domains **New**

Workloads

Capacity settings

Refresh summary

Embed Codes

Organizational visuals

Azure connections

Workspaces

Custom branding

Protection metrics

Fabric identities

Featured content

Help + support

Developer settings

- ▷ Embed content in apps
Enabled for the entire organization
- ▾ Service principals can use Fabric APIs
Unapplied changes

Web apps registered in Microsoft Entra ID can use service principals, rather than user credentials, to authenticate to Fabric APIs. To allow an app to use a service principal as an authentication method, the service principal must be added to an allowed security group. [Learn More](#)

Enabled

🛡️ Service principals can use APIs to access tenant-level features controlled by Fabric admins and enabled for the entire organization or for security groups they're included in. You can control access of service principals by creating dedicated security groups for them and using these groups in any Fabric tenant level-settings. [Learn More](#)

Apply to:

The entire organization

Specific security groups

Enter security groups

Specify at least one security group.

Now you can access the non-admin Power BI REST API endpoints like <https://api.powerbi.com/v1.0/myorg/groups>

In order to also be able to access the admin Power BI REST API endpoints like

[https://api.powerbi.com/v1.0/myorg/admin/groups?\\$top=100](https://api.powerbi.com/v1.0/myorg/admin/groups?$top=100)

You will need to allow the app to use a service principal instead of user credentials in order to authenticate. This can be done by enabling the setting below.

Admin portal

- Tenant settings
- Usage metrics
- Users
- Premium Per User
- Audit logs
- Domains New
- Workloads
- Capacity settings
 - Refresh summary
- Embed Codes
- Organizational visuals
- Azure connections
- Workspaces
- Custom branding
- Protection metrics
- Fabric identities

Admin API settings

- Service principals can access read-only admin APIs *Unapplied changes*

Web apps registered in Microsoft Entra ID can use service principals, rather than user credentials, to authenticate to read-only admin APIs.

To allow an app to use a service principal as an authentication method, the service principal must be added to an allowed security group. Service principals included in allowed security groups will have read-only access to all the information available through admin APIs, which can include users' names and emails, and detailed metadata about semantic models and reports. [Learn More](#)

Enabled

Apply to:

- The entire organization
- Specific security groups

Enter security groups

Specify at least one security group.

Now you can start doing API calls by getting the groups (workspaces) for example

Set the authentication for these API calls to Bearer Token and use your recently acquired Bearer Token

[https://api.powerbi.com/v1.0/myorg/admin/groups?\\$top=100](https://api.powerbi.com/v1.0/myorg/admin/groups?$top=100)