

Service Principal to Call Power BI REST API

Azure AD Setup

Step 1: Register an App in Microsoft Entra ID

1. **Sign in to the Azure Portal** (portal.azure.com) with an account that has permission to create app registrations.
2. Navigate to **Microsoft Entra ID > App registrations** and select **New registration**.
3. Configure the app:
 - **Name:** Enter a meaningful name (for example, [PBI_REST_API_App](#)).
 - **Supported account types:** Select **Accounts in this organizational directory only** for a single-tenant app.
 - **Redirect URI:** This is optional for service principals. You can leave it blank or select **Web** and enter a placeholder such as <https://localhost>.
4. Click **Register** to complete the app registration.
5. From the app's **Overview** page, record the following:
 - **Application (client) ID**
 - **Directory (tenant) ID**

Step 2: Create a Client Secret

1. In the app settings, go to **Certificates & secrets > Client secrets** and select **New client secret**.
2. Enter a description (for example, [PBI_API_Secret](#)) and set an expiration period (for example, 36 months). **Note:** Track the expiration date, as the client secret must be renewed before it expires.
3. Click **Add**, then copy the **secret value** immediately. The value is displayed only once.
4. **Best practice:** Store the client secret securely in **Azure Key Vault** instead of hardcoding it in scripts.

Step 3: Create a Security Group

1. In the Azure Portal, go to **Microsoft Entra ID > Groups** and select **New group**.
2. Configure the group:
 1. **Group type:** Security
 2. **Group name:** For example, [PBI_Service_Principal_Security_Group](#)
 3. **Group description:** Add a clear description for future reference.
3. Add the service principal as a member. Click **No members selected**, search for the app by name, select it, and click **Select**.

4. Click **Create**.

Step 4: Configure Power BI Admin Settings

1. Sign in to the **Power BI Admin Portal** (app.powerbi.com/admin-portal) with a Power BI administrator account.
2. Go to **Tenant settings > Developer settings** and locate **Allow service principals to use Power BI APIs**.
3. Enable the setting and select **Specific security groups**.
4. Add the security group created in Step 3 (for example, [PBI_Service_Principal_Security_Group](#)) and click **Apply**.
5. If you are using admin APIs, enable **Allow service principals to use read-only admin APIs** under **Admin API settings** and apply the setting to the same security group.

Step 5: Grant Workspace Access

1. In the Power BI service, navigate to the target workspace.
2. Select **More > Workspace access**.
3. Search for the service principal using the app's display name, select it, and assign an appropriate role, such as **Admin** or **Member**.
4. Click **Add**.

Profit.co Configuration

During the Profit.co configuration, you need the **Client ID**, **Client Secret**, and **Tenant ID**. These credentials are used to authenticate the service principal and call the Power BI REST API to retrieve the required response.