Speaker availability - o365

To set up the “Speaker availability“ feature, the following data points need to be provided:

```
clientId
tenantId
clientSecret
```

Authentication and authorization steps

The basic steps required to configure a service and get a token from the Microsoft identity platform endpoint that your service can use to call Microsoft Graph under its own identity are:

1. Register your app.
2. Configure permissions for Microsoft Graph on your app.
3. Get administrator consent.
4. Create client secret

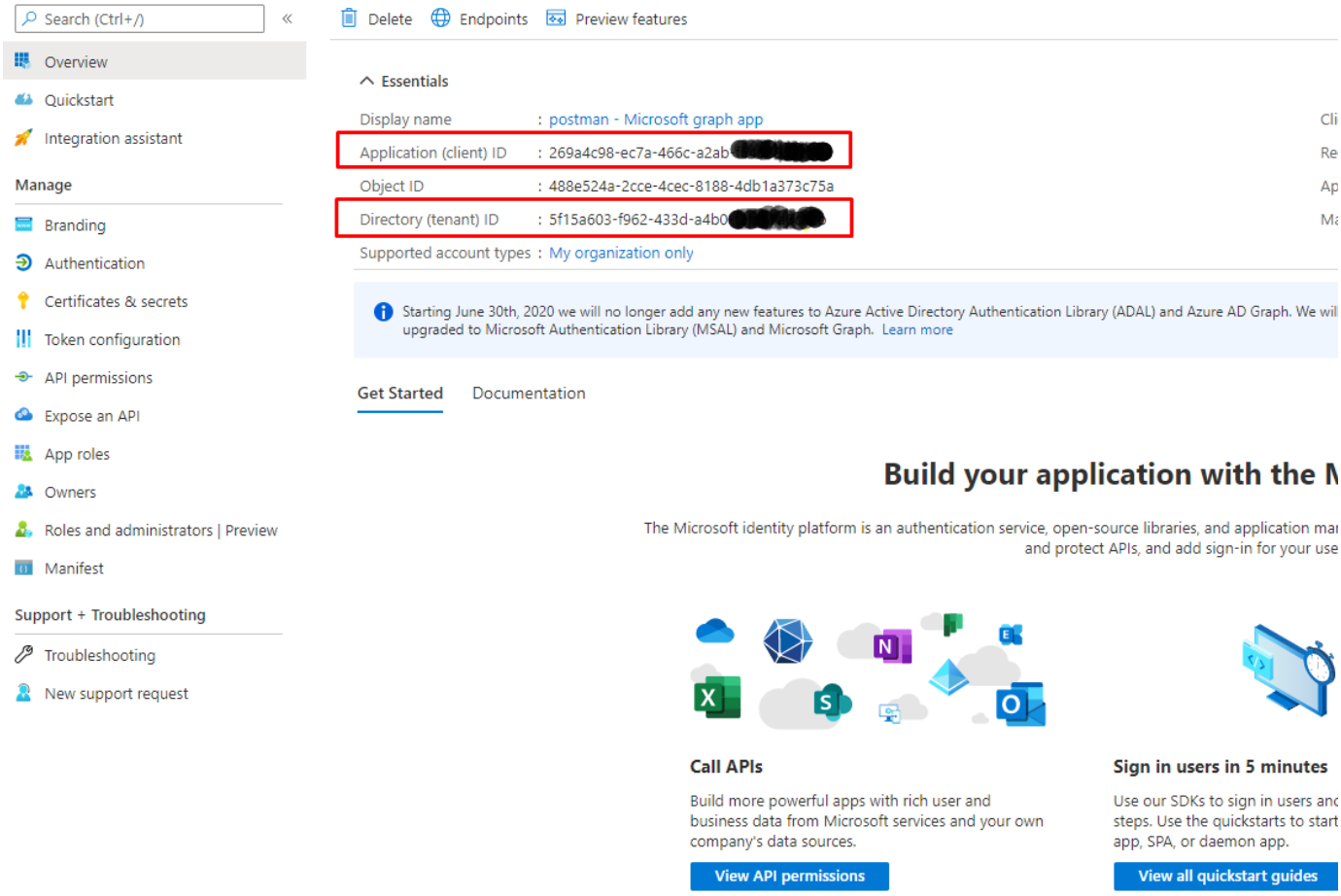
1. Register your app

To authenticate with the Microsoft identity platform endpoint, you must first register your app at the Azure app registration portal. You can use either a Microsoft account or a work ~~or school~~ account to register your app.

For a service that will call Microsoft Graph under its own identity, you need to register your app for the Web platform and copy the following values:

- The Application ID assigned by the Azure app registration portal.
- A Client (application) Secret, either a password or a public/private key pair (certificate).
- A Redirect URL for your service to receive token responses (not necessarily)
- A Redirect URL for your service to receive admin consent responses if your app implements functionality to request administrator consent. (not necessarily)

For steps on how to configure an app using the Azure app registration portal, see Register your app.

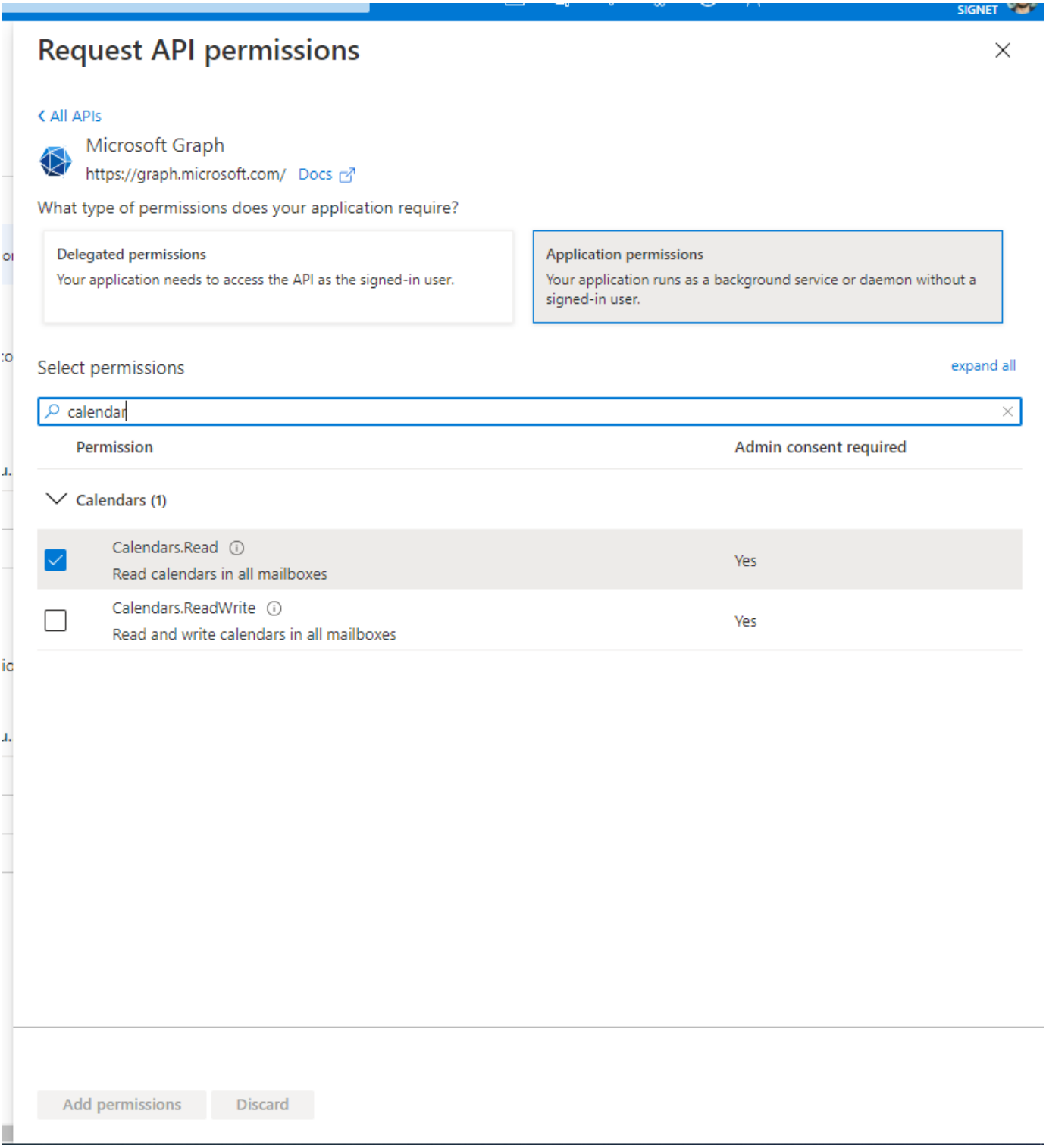


2. Configure permissions for Microsoft Graph

To configure application permissions for your app in the Azure app registrations portal: under an application's **API permissions** page, choose **Add a permission**, select **Microsoft Graph**, and then choose the permissions your app requires under **Application permissions**.

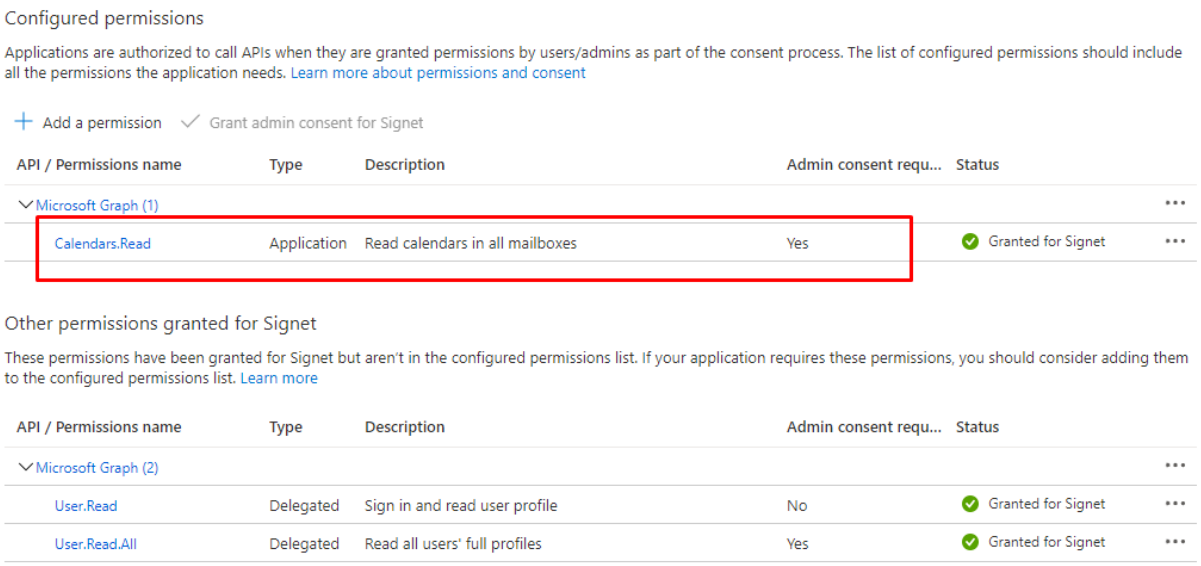
The following screenshot shows the **Select Permissions** dialog box for Microsoft Graph application permissions.

Select “Calendars.Read“



3. Administrator consent experience

You can rely on an administrator to grant the permissions your app needs at the Azure portal; however, often, a better option is to provide a sign-up experience for administrators by using the Microsoft identity platform `/adminconsent` endpoint.



4. Create client secret

1. From **App registrations** in Azure AD, select your application.
2. Select **Certificates & secrets**.
3. Select **Client secrets -> New client secret**.
4. Provide a description of the secret, and a duration. When done, select **Add**.

   After saving the client secret, the value of the client secret is displayed. Copy this value because you won't be able to retrieve the key later. You will provide the key value with the application ID to sign in as the application. Store the key value where your application can retrieve it.