Authorization Server Administration Guide

# Applications

The main purpose of this document is to describe manage and register internal applications to the Authorization server (the System) for the authentication process (SSO).

It also provides guide and overview of applications management processes such as registration, enabling/disabling SSO provider support, parameters modification and complete removal from the System.

## Add application

1. In the dashboard with applications table click on the Add button.

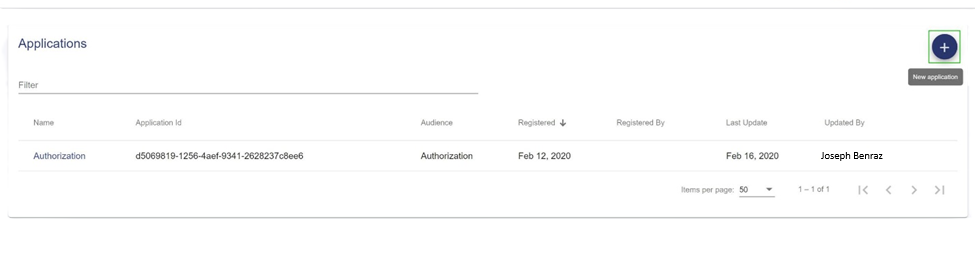


Figure 1. Add a new application

1. Fill in all the application properties:
   * Name = {Name of the application};
   * Exchange claims URL = {URL for exchanging claims, provided by application’s team};
   * Callback URL = {URL for callbacks with access token or error message, provided by application’s team}.

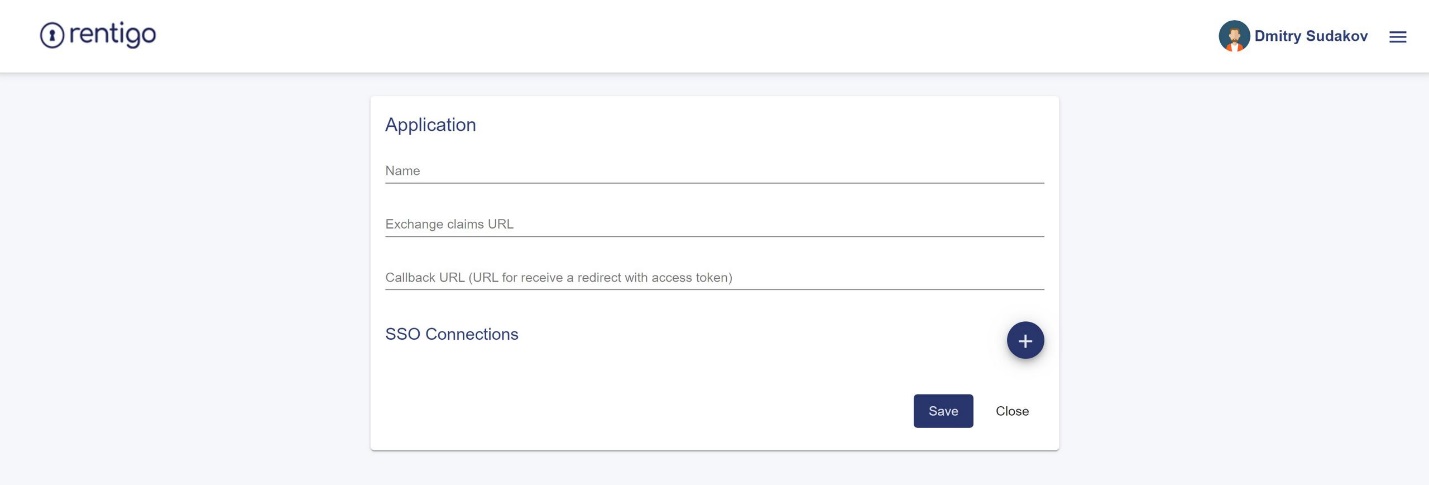


Figure 2. Fill in parameters of a new application

1. Click on Save button and confirm the operation.

## Modify application parameters

To modify one or several application parameters such as Name or Callback URL:

1. In the dashboard with applications table find the application and open application form by clicking on application’s name link.

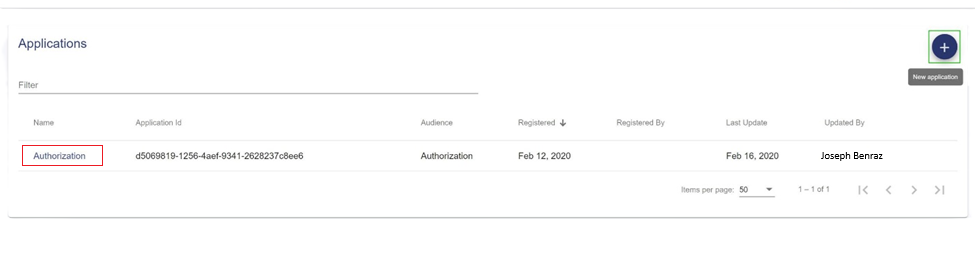


Figure 3. Select application to modify

1. Modify desired application parameters.
2. Click on Save button and confirm the operation.

## Modify application SSO connections

### Add Microsoft SSO connection

#### Register application in Microsoft Azure AD

1. Go to [https://portal.azure.com](https://portal.azure.com/) -> Azure Active Directory -> App registration.
2. Press New registration button.

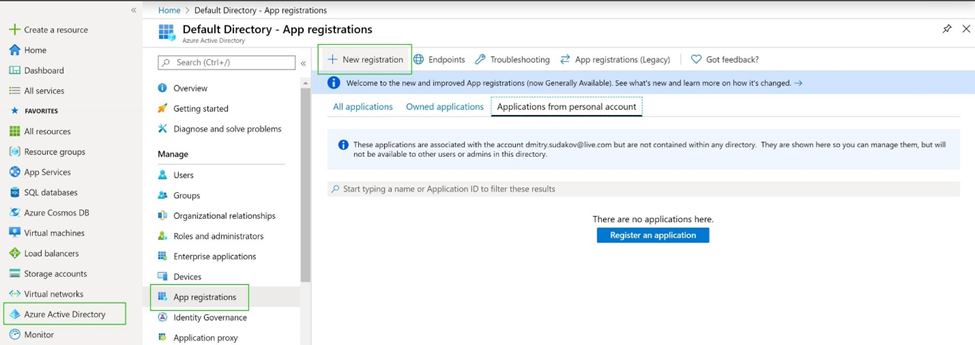


Figure 4. Azure AD – select new application registration

1. Enter name of new application, select supported account types (depends on the needs) and redirect URI of type Web and value of Microsoft callback endpoint.

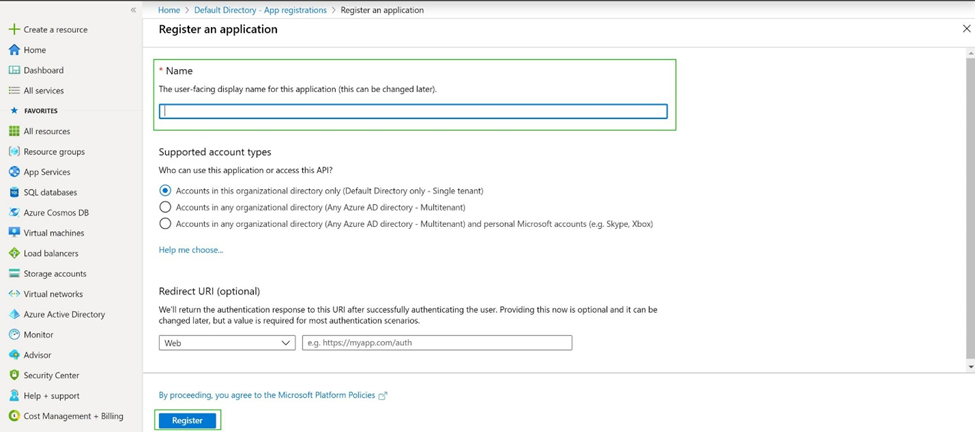


Figure 5. Azure AD – fill in new application name and redirect URL

1. Add application API permissions for User.Read and Group.Read.All and grant them Admin Consent in Azure Active Directory -> App registrations -> {Application Name} -> API permissions.
   1. Open API permissions and click on Add a permission.

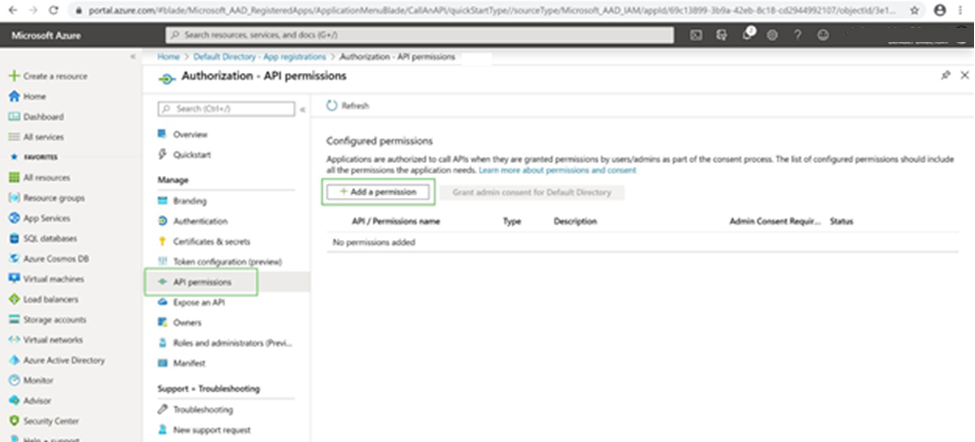


Figure 6. Azure AD – add application permissions

* 1. Select Microsoft Graph.

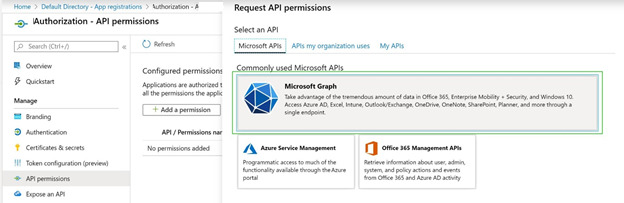


Figure 7. Azure AD – select Microsoft Graph

* 1. Select Delegated permissions.

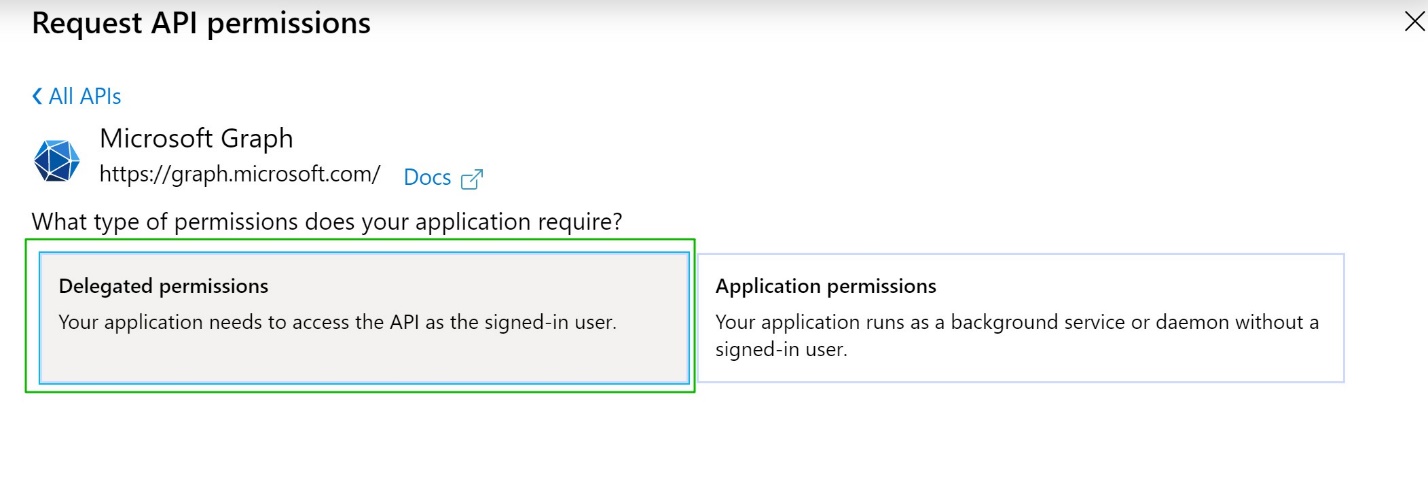


Figure 8. Azure AD – select Delegated permissions

* 1. Check User.Read and Group.Read.All and click Add permissions.

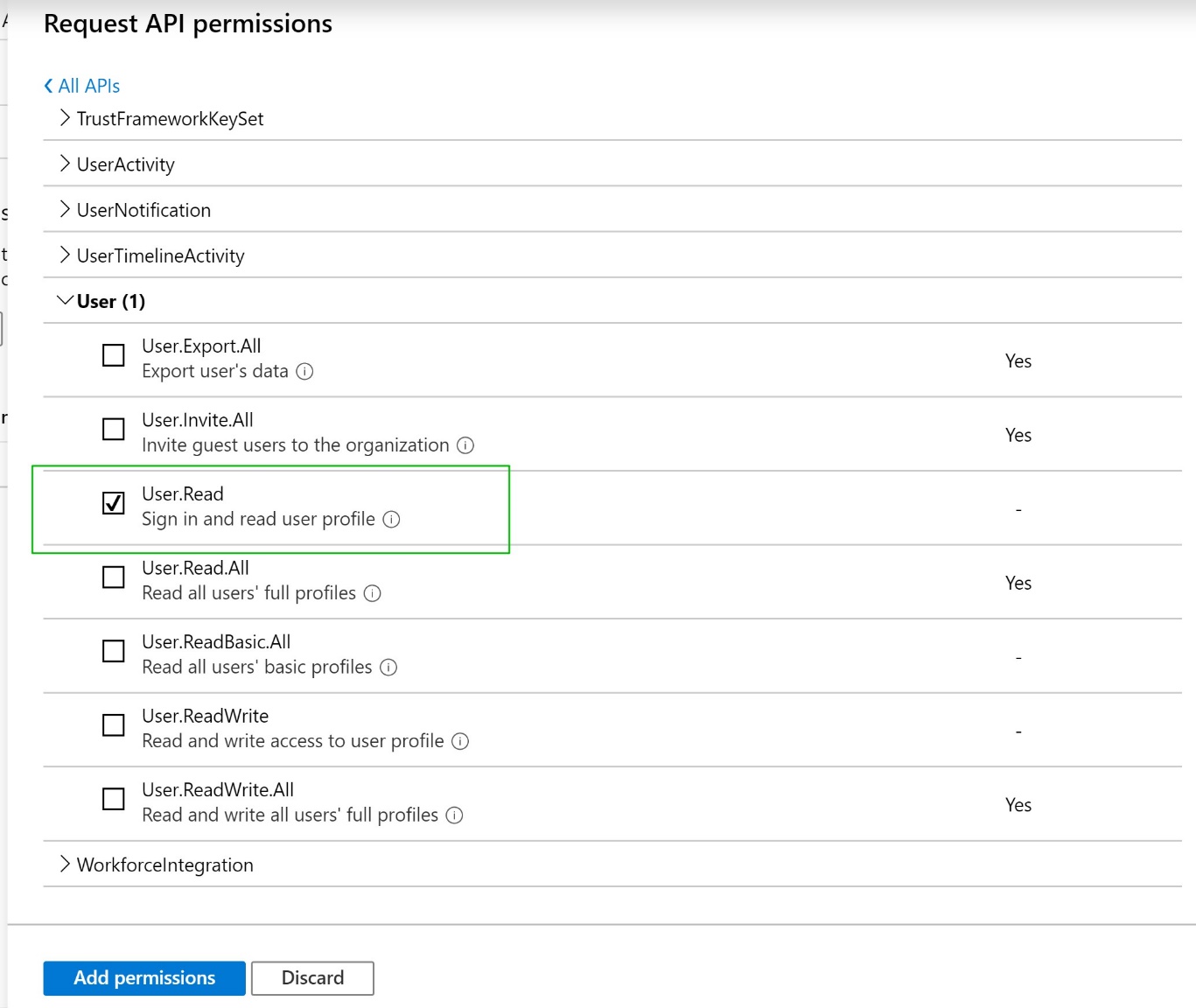


Figure 9. Azure AD – check User.Read

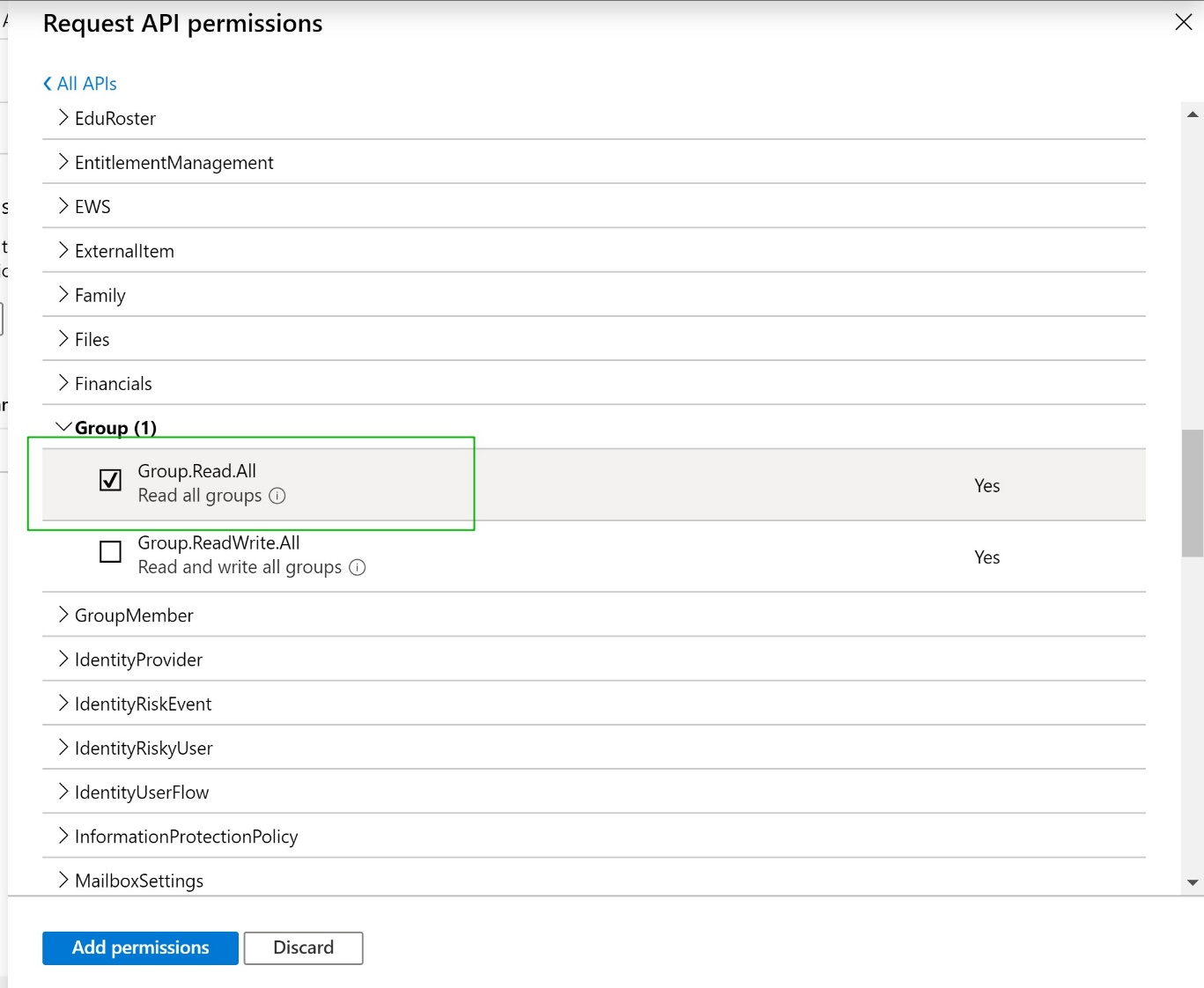


Figure 10. Azure AD – check Group.Read.All

* 1. Grant admin consent.

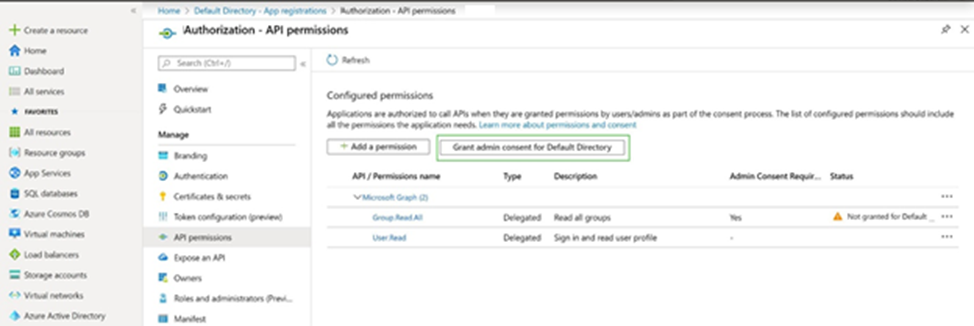


Figure 11. Azure AD – grant admin consent

1. Add the users and/or groups that are allowed to use the application in Enterprise applications -> All applications -> {Application Name} -> Users and groups.

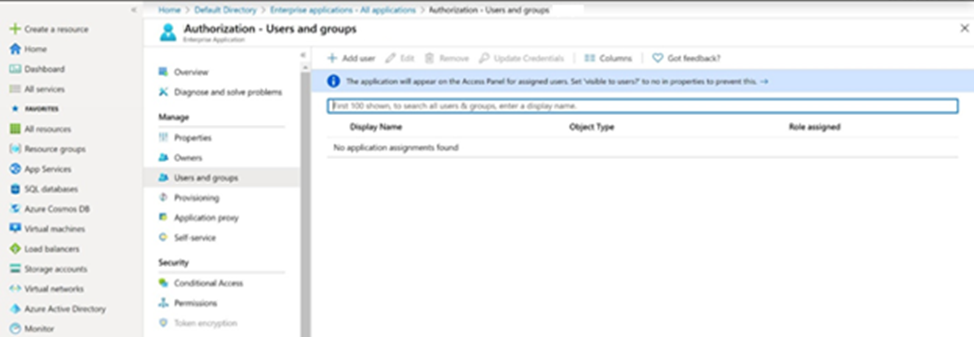


Figure 12. Azure AD – application users and groups management

1. Get Directory (Tenant Id) and Application (Client Id) of the application from Azure Active Directory -> App registrations -> {Application Name} -> Overview. They will be used in new SSO connection.

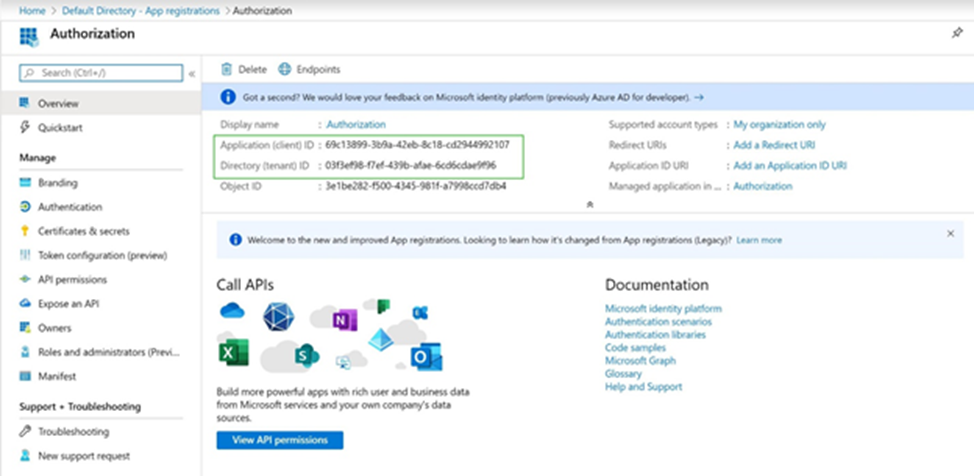


Figure 13. Azure AD – application parameters

1. Generate and preserve new secret for the application in Azure Active Directory -> App registrations -> {Application Name} -> Certificates and secrets. It also will be used in new SSO connection.

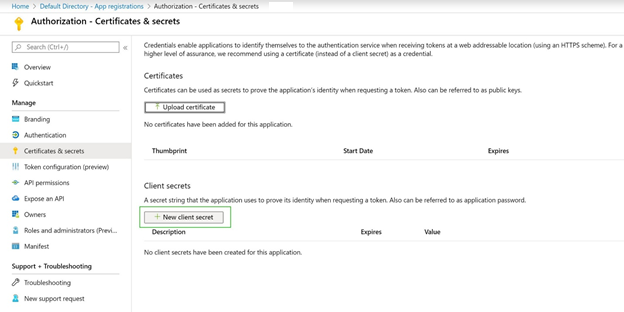


Figure 14. Azure AD – client secret generation

#### Add SSO connection in UI

1. Go to applications table and open application edit form.
2. Click on Add SSO connection and select “Microsoft”.

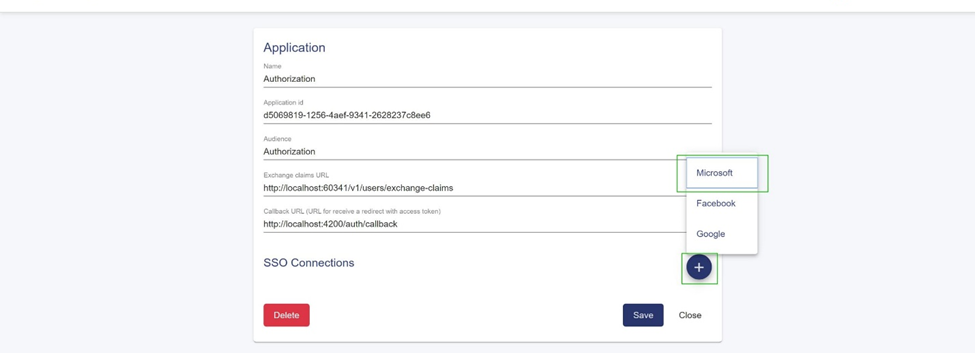


Figure 15. Add Microsoft SSO connection

1. Fill in all SSO connection parameters:

* AuthorizationUrl = [https://login.microsoftonline.com/{tenant-id}/oauth2/v2.0/authorize](https://login.microsoftonline.com/%7btenant-id%7d/oauth2/v2.0/authorize);
* TokenUrl = [https://login.microsoftonline.com/{tenant-id}/oauth2/v2.0/token](https://login.microsoftonline.com/%7btenant-id%7d/oauth2/v2.0/token);
* ClientId = {Client Id};
* ClientSecret = {Client secret};
* Scope = user.read group.read.all;
* Enabled = Yes.

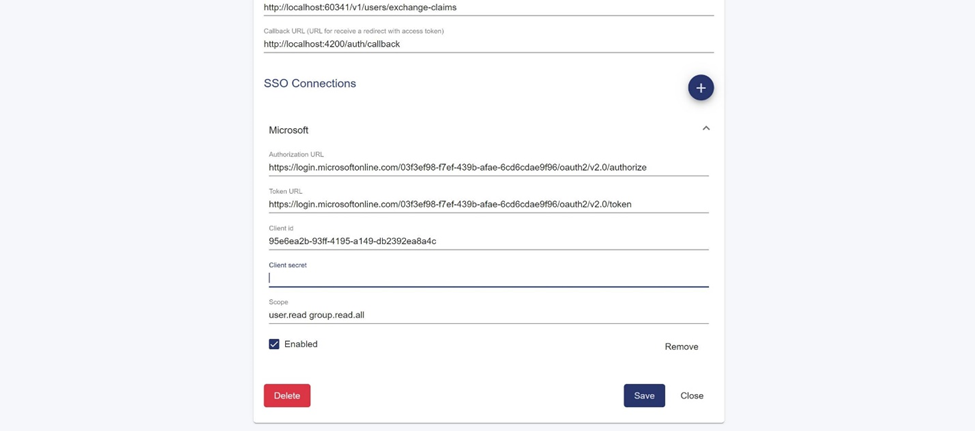


Figure 16. Fill in Microsoft SSO connection parameters

1. Click on Save button and confirm the operation.

### Add Facebook SSO connection

#### Register application in Facebook

1. Go to <https://developers.facebook.com>, open My Apps menu and press Create App.

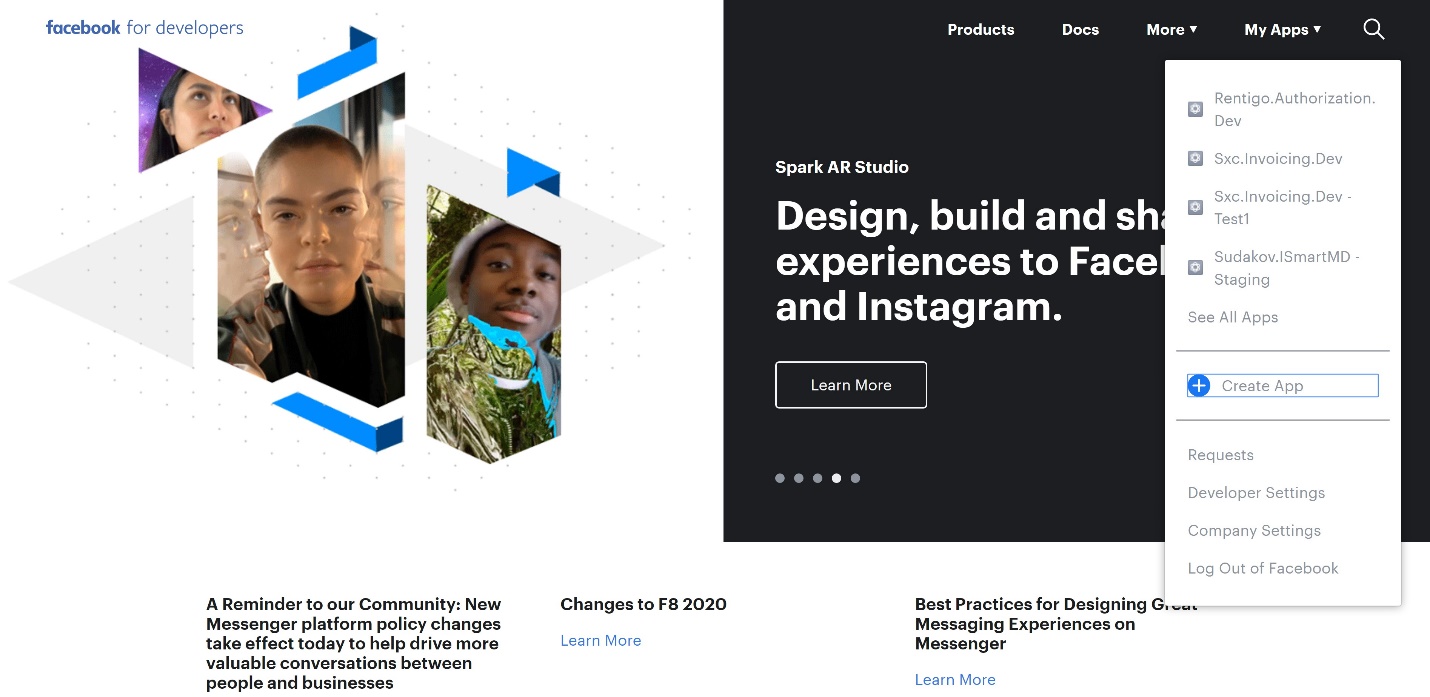


Figure 17. Facebook – create new app

1. Fill Display Name and Contact Email, press Create App ID.

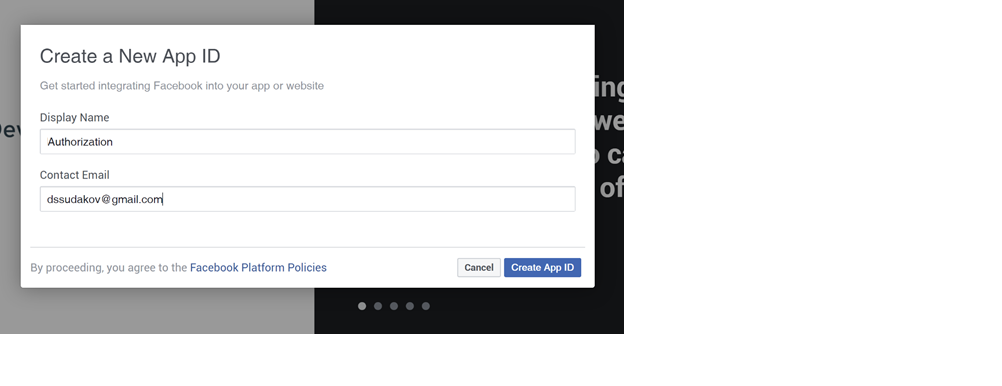


Figure 18. Facebook – fill in Display name and Contact Email

1. Add Facebook Login product.

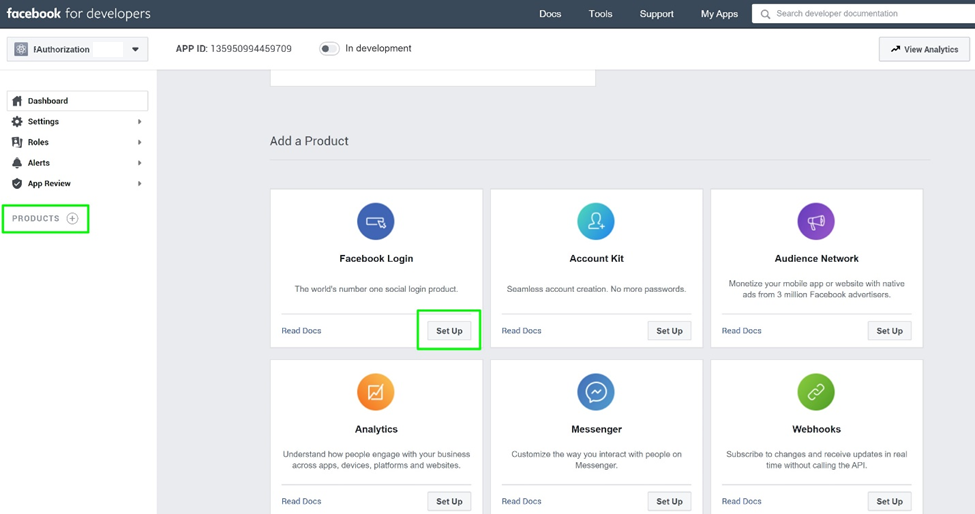


Figure 19. Facebook – add Facebook Login product

1. Add to Valid OAuth Redirect URLs URL for receiving Facebook callbacks (for localhost URLs this field could be kept blank).

Redirect URIs example: http://authorization**.{env}.**benraz.com/v1/auth/facebook-callback

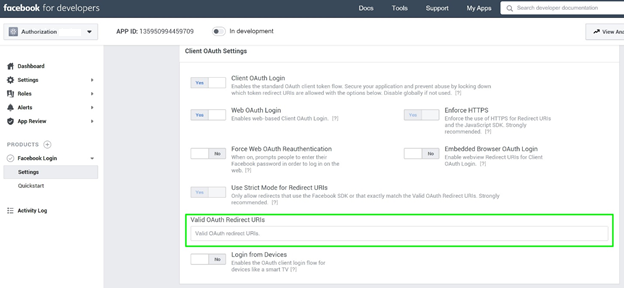


Figure 20. Facebook – fill in Redirect URLs

1. Get App ID and App Secret from Settings -> Basic. They will be used in new SSO connection.

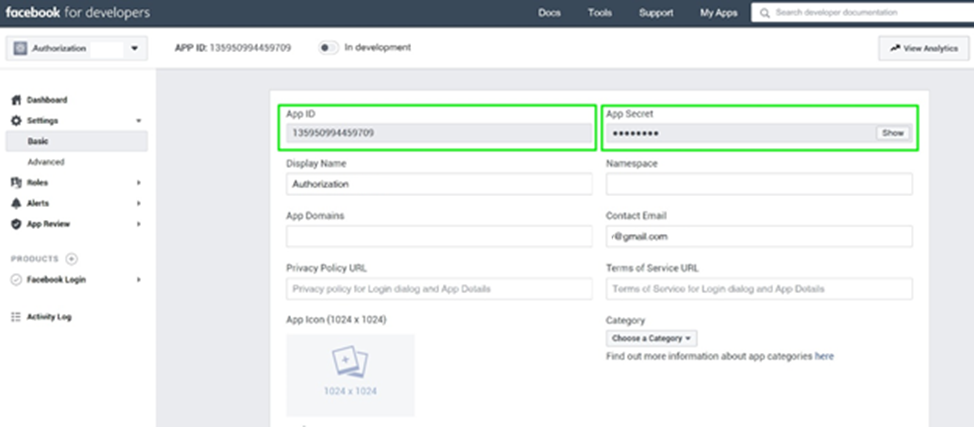


Figure 21. Get App ID and App Secret

#### Add SSO connection in UI

1. Go to applications table and open application edit form.
2. Click on Add SSO connection and select “Facebook”.

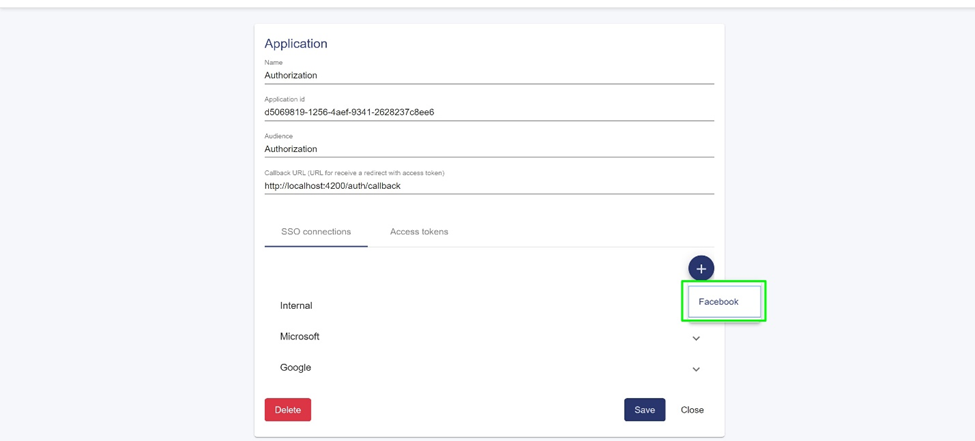


Figure 22. Add Facebook SSO connection

1. Fill in all SSO connection parameters:

* AuthorizationUrl = https://www.facebook.com/v6.0/dialog/oauth;
* TokenUrl = https://graph.facebook.com/v6.0/oauth/access\_token;
* ClientId = {App ID};
* ClientSecret = {App Secret};
* Scope = email;
* Enabled = Yes.

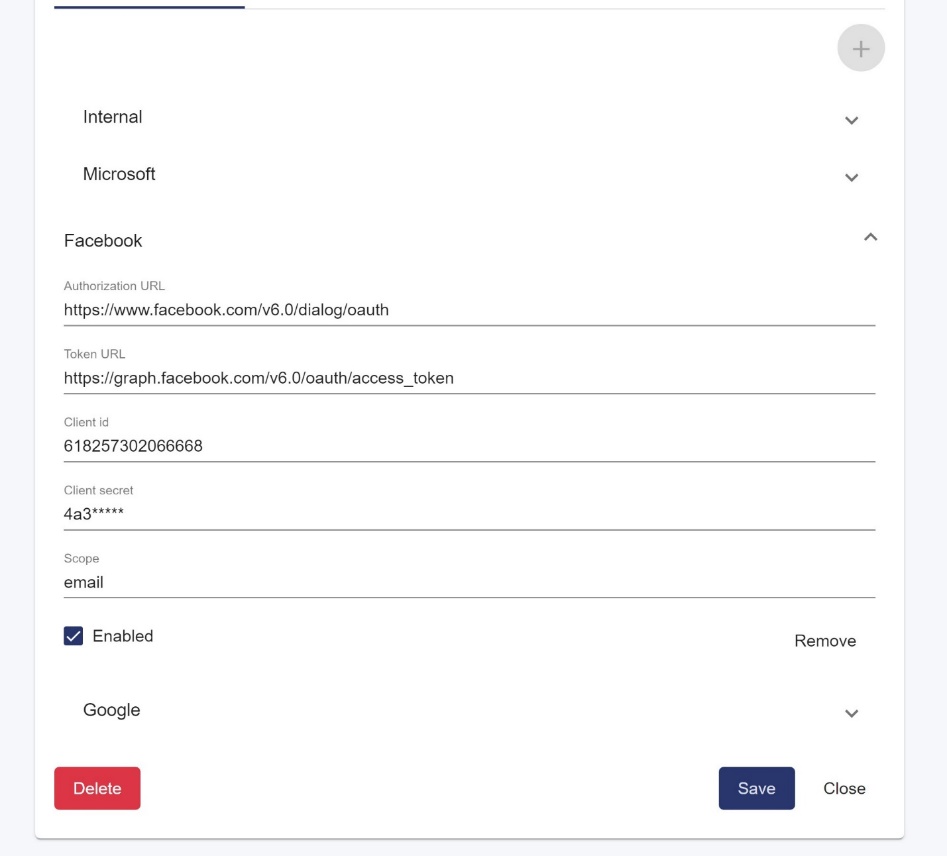


Figure 23. Fill in Facebook SSO connection parameters

1. Click on Save button and confirm the operation.

### Add Google SSO connection

#### Register application in Google

1. Go to <https://console.developers.google.com>.
2. Add new project if needed (there is no project or you want a new one for this particular application).

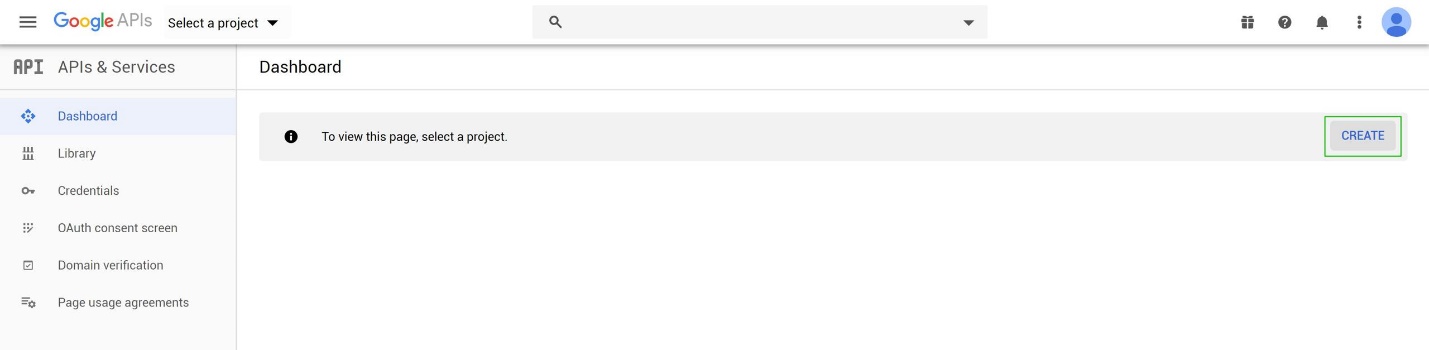


Figure 24. Google – create new project

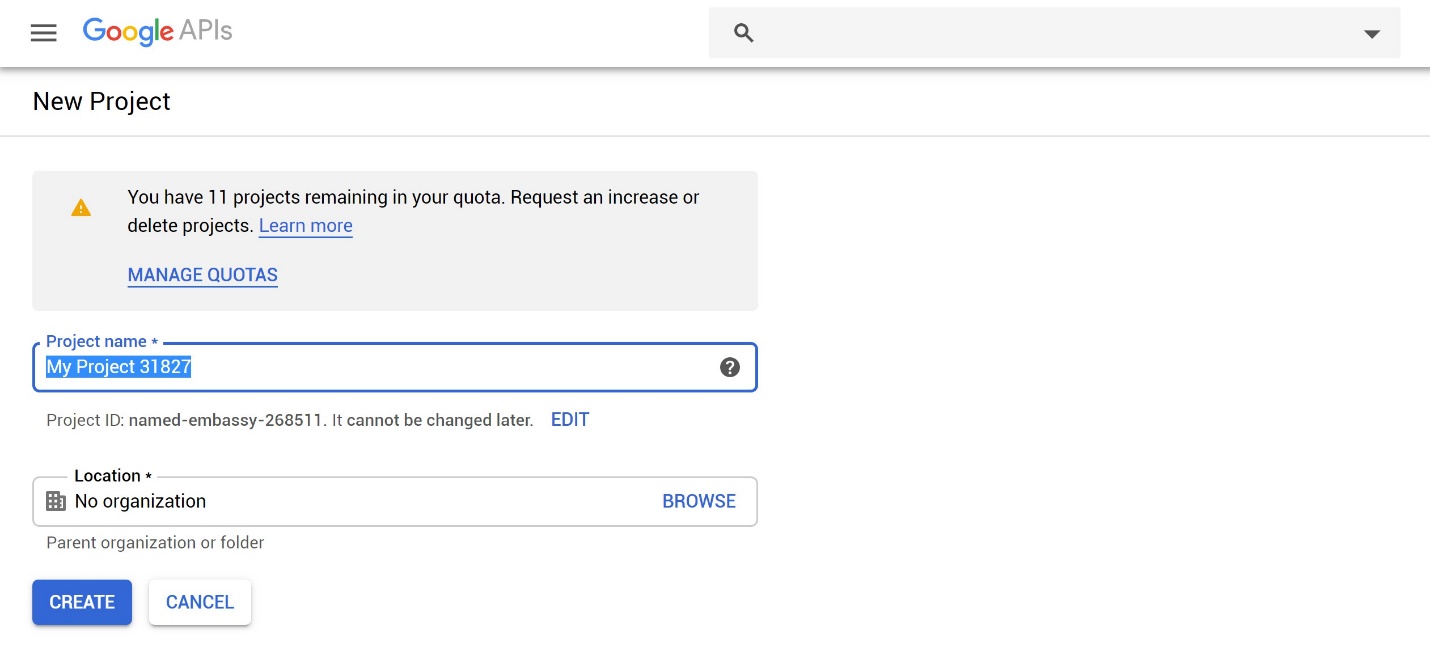


Figure 25. Google – fill in new project parameters

1. Add OAuth consent screen, selecting external consent and setting up application name; all the other parameters such as application logo are optional.

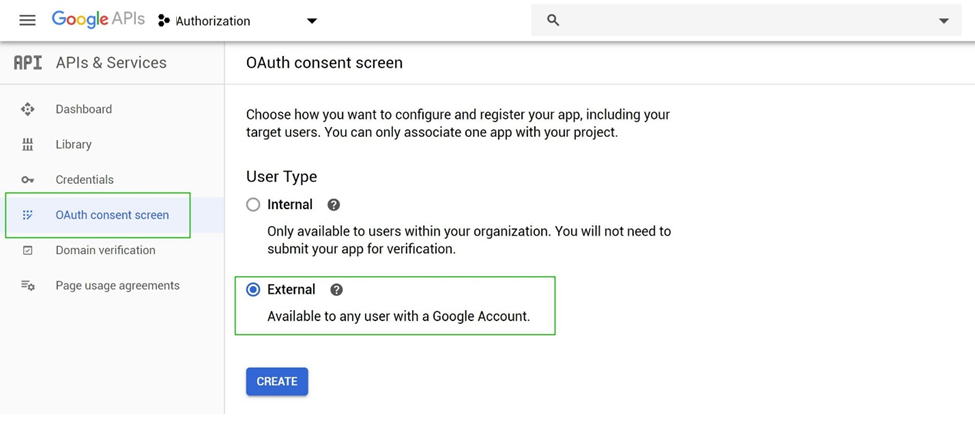


Figure 26. Google – add new consent screen

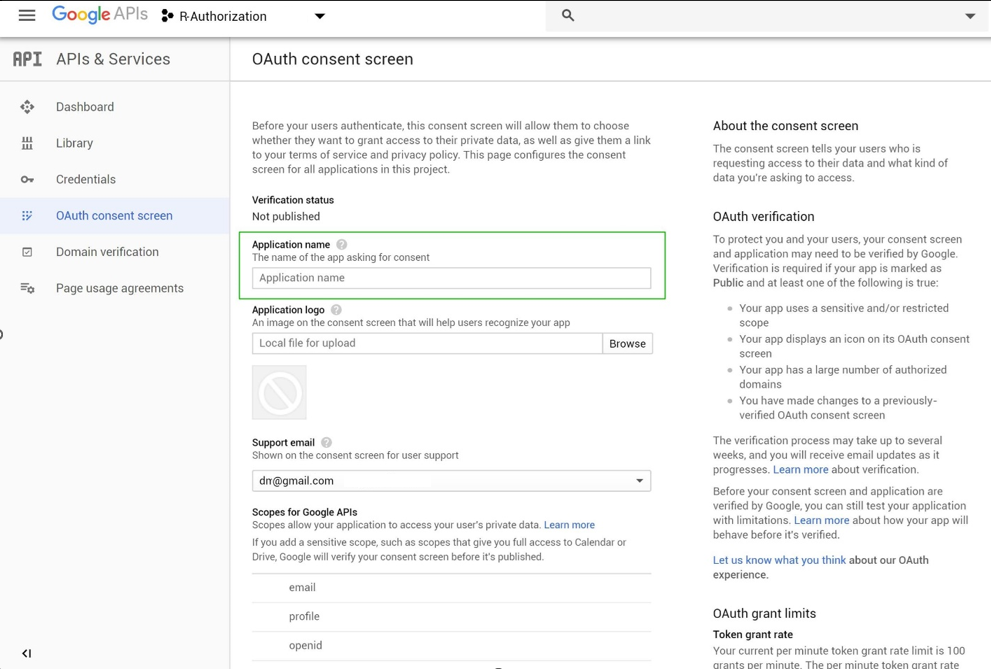


Figure 27. Google – fill in new consent screen parameters

1. Add new credentials:
   1. Select “Create credentials” on “Credentials” tab, choose “OAuth Client ID” in a dropdown menu.

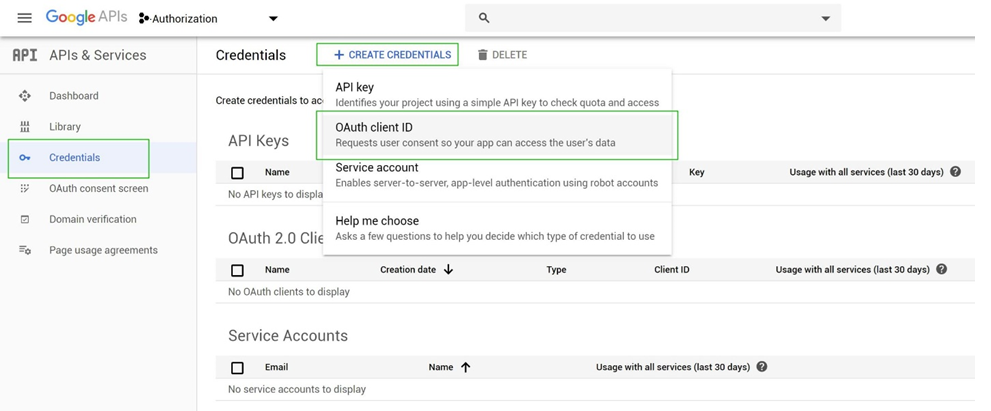


Figure 28. Google – create new credentials

* 1. Choose “Web application” in an options group, fill in Name = {Desired application name} and Authorised redirect URIs = {URL of google callback endpoint, configured in Auth server}.

redirectURI example: http://authorization**.{env}.**benraz.com/v1/auth/google-callback

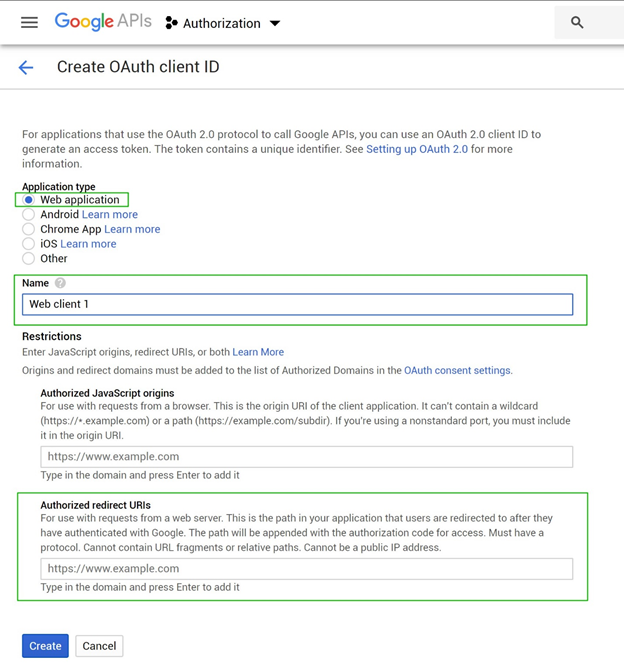


Figure 29. Google – fill in new OAuth client parameters

* 1. Click Save.

1. Notice Client ID and Client secret, they will be used in new SSO connection.

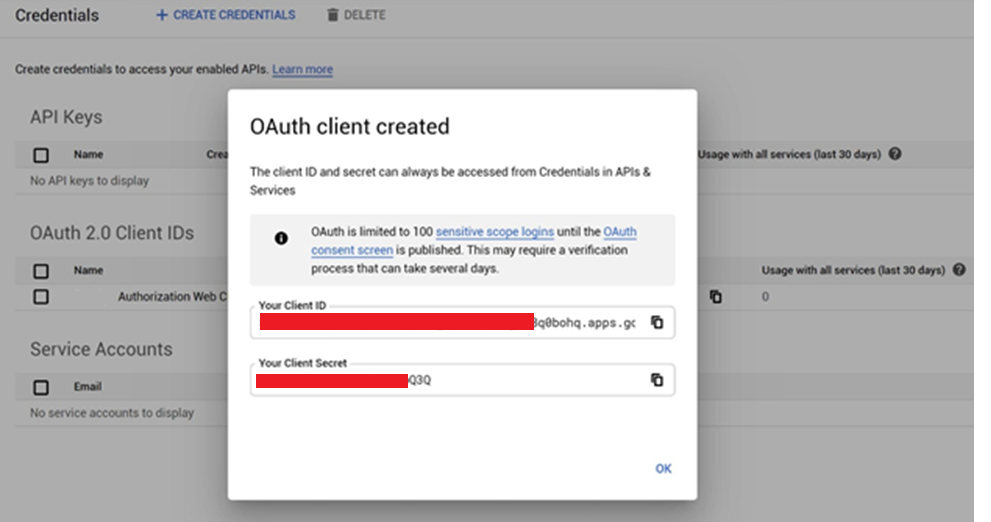


Figure 30. Google – client created

#### Add SSO connection in UI

1. Go to applications table and open application edit form.
2. Click on Add SSO connection and select “Google”.

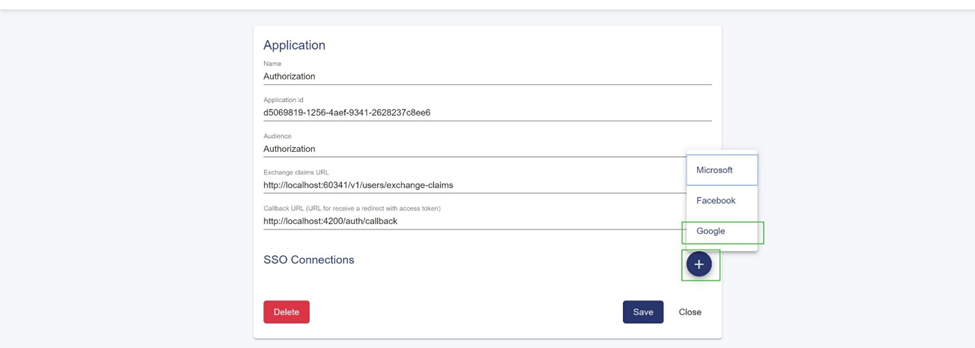


Figure 31. Add Google SSO connection

1. Fill in all SSO connection parameters:

* AuthorizationUrl = <https://accounts.google.com/o/oauth2/v2/auth>;
* TokenUrl = <https://oauth2.googleapis.com/token>;
* ClientId = {Client Id};
* ClientSecret = {Client secret};
* Scope = openid profile email;
* Enabled = Yes.

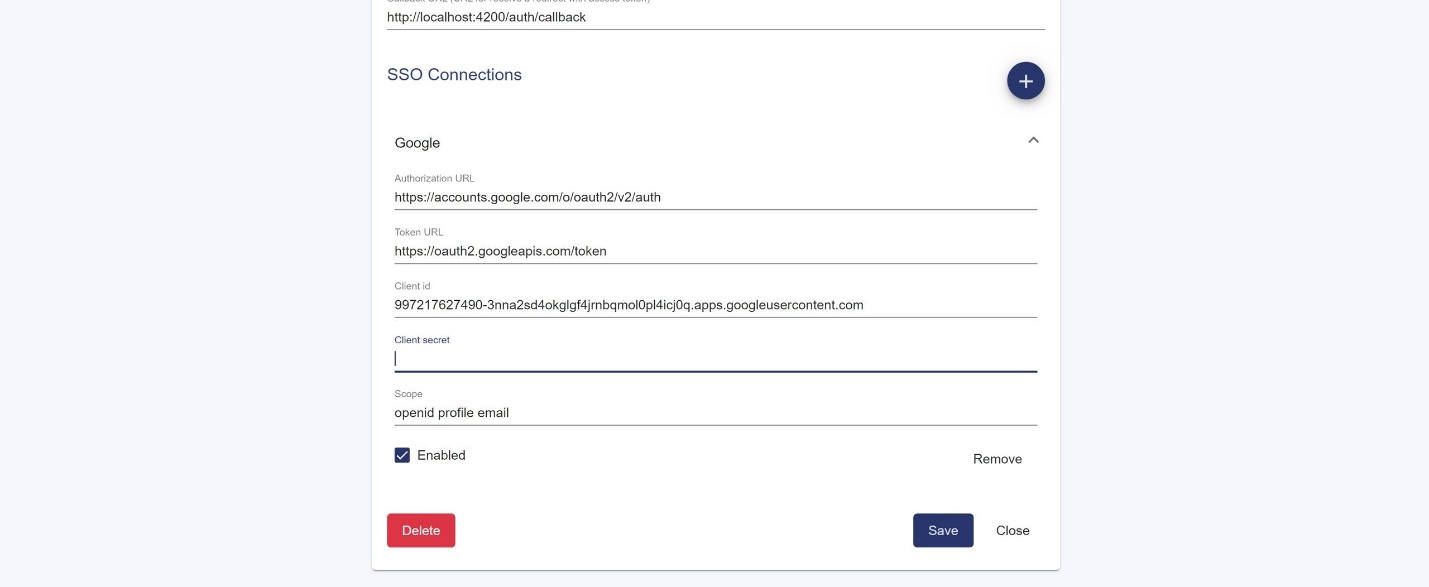


Figure 32. Fill in Google SSO connection parameters

1. Click on Save button and confirm the operation.

### Enable/disable SSO connection

1. Go to applications table and open application edit form.
2. Expand desired SSO connection.

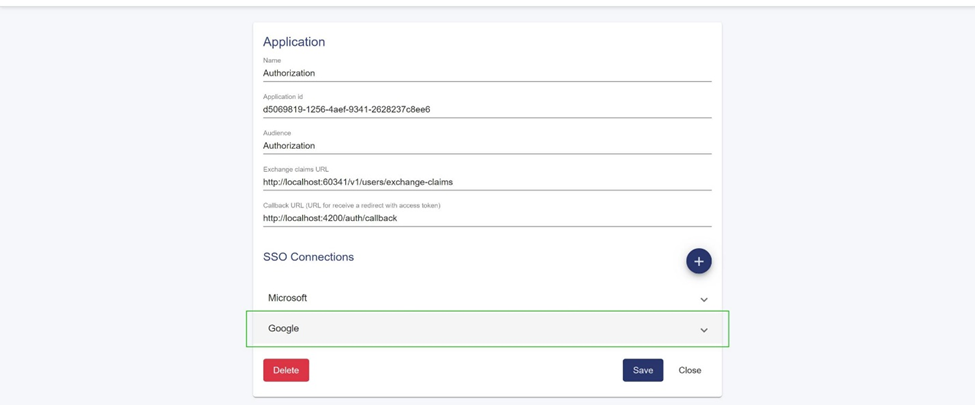


Figure 33. Application SSO connections

1. Check/uncheck Enabled checkbox for the SSO connection.

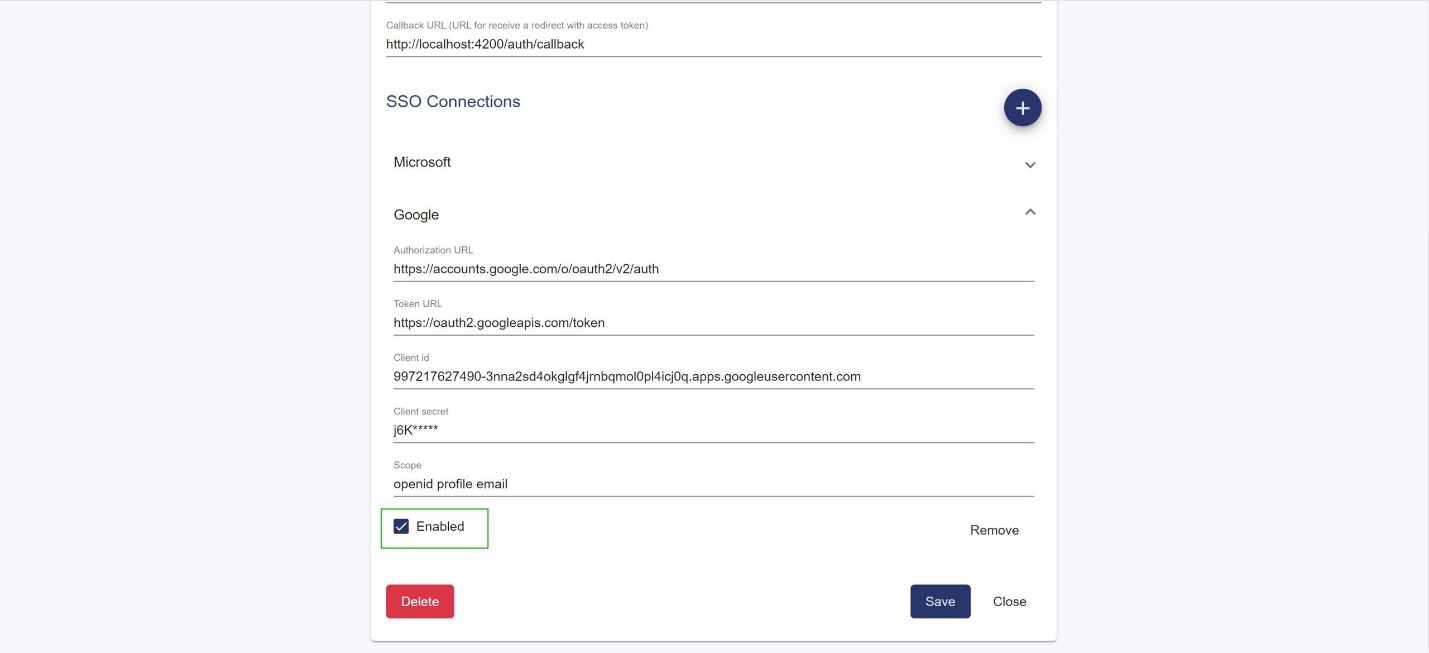


Figure 34. Application SSO connection Enabled flag

1. Click on Save button and confirm the operation.

### Remove SSO connection

1. Go to applications table and open application edit form.
2. Expand desired SSO connection.
3. Click on Remove button in expanded SSO connection details form.

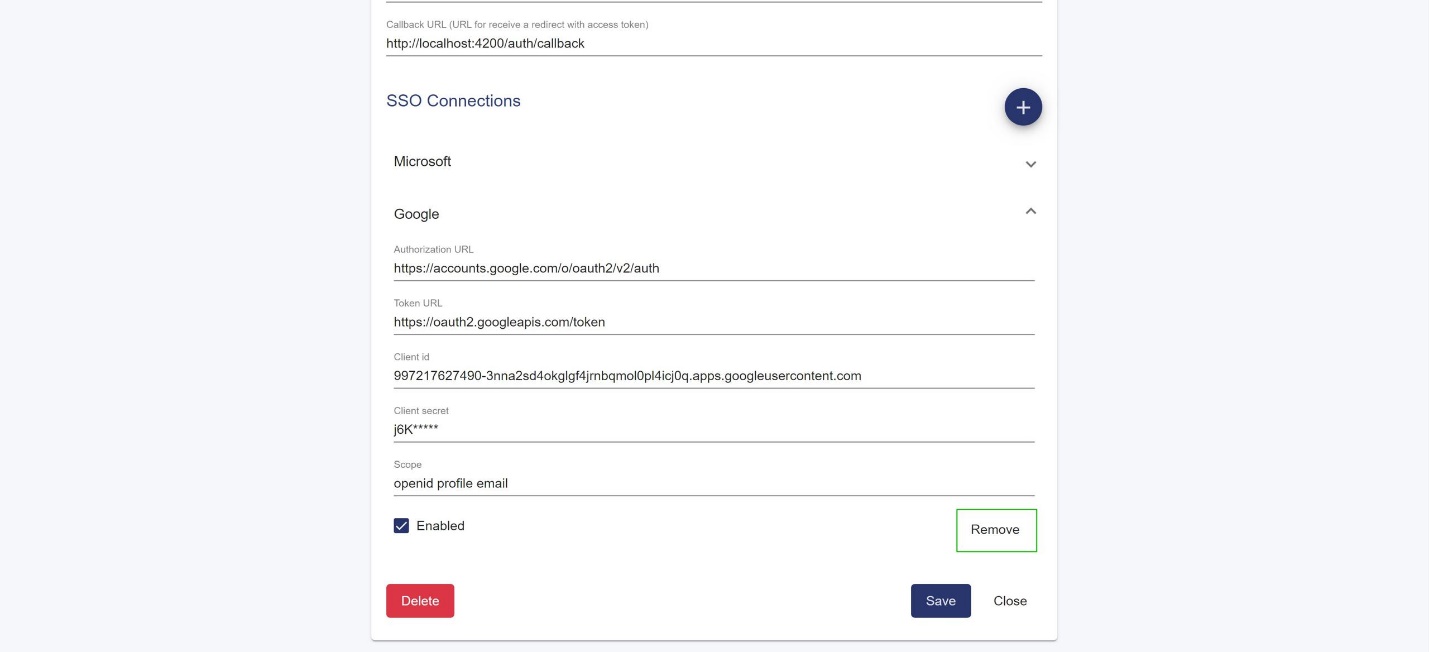


Figure 35. Remove application SSO connection

1. Click on Save button and confirm the operation.

## Remove application

1. Go to applications table and open application edit form.
2. Click on Delete button and confirm the operation.

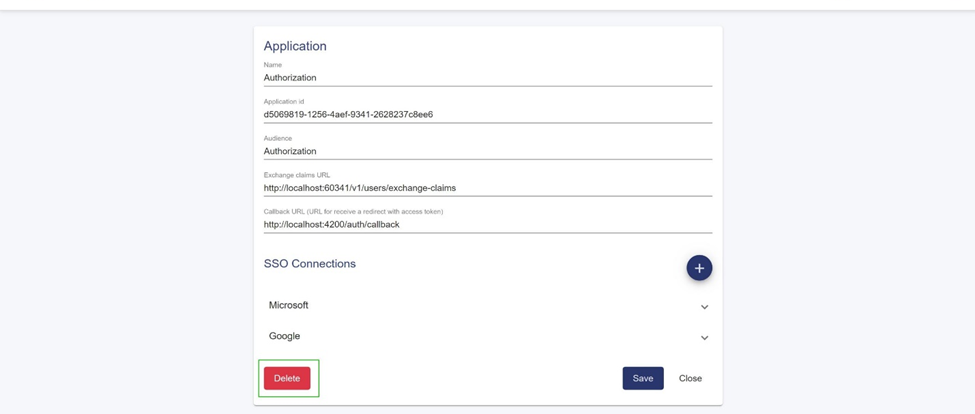


Figure 36. Delete application

# Users

# Roles & Claims