



Primero Guidance on Federating to B2C

There are 2 types of processes we follow to set up single-sign on with partners. The first process is for partners' who have a Google underlying identity provider. The second process is for non-Google providers, such as Entra ID (formerly Azure Active Directory).

This guidance outlines the process for partners who use Entra ID.

Step 1:

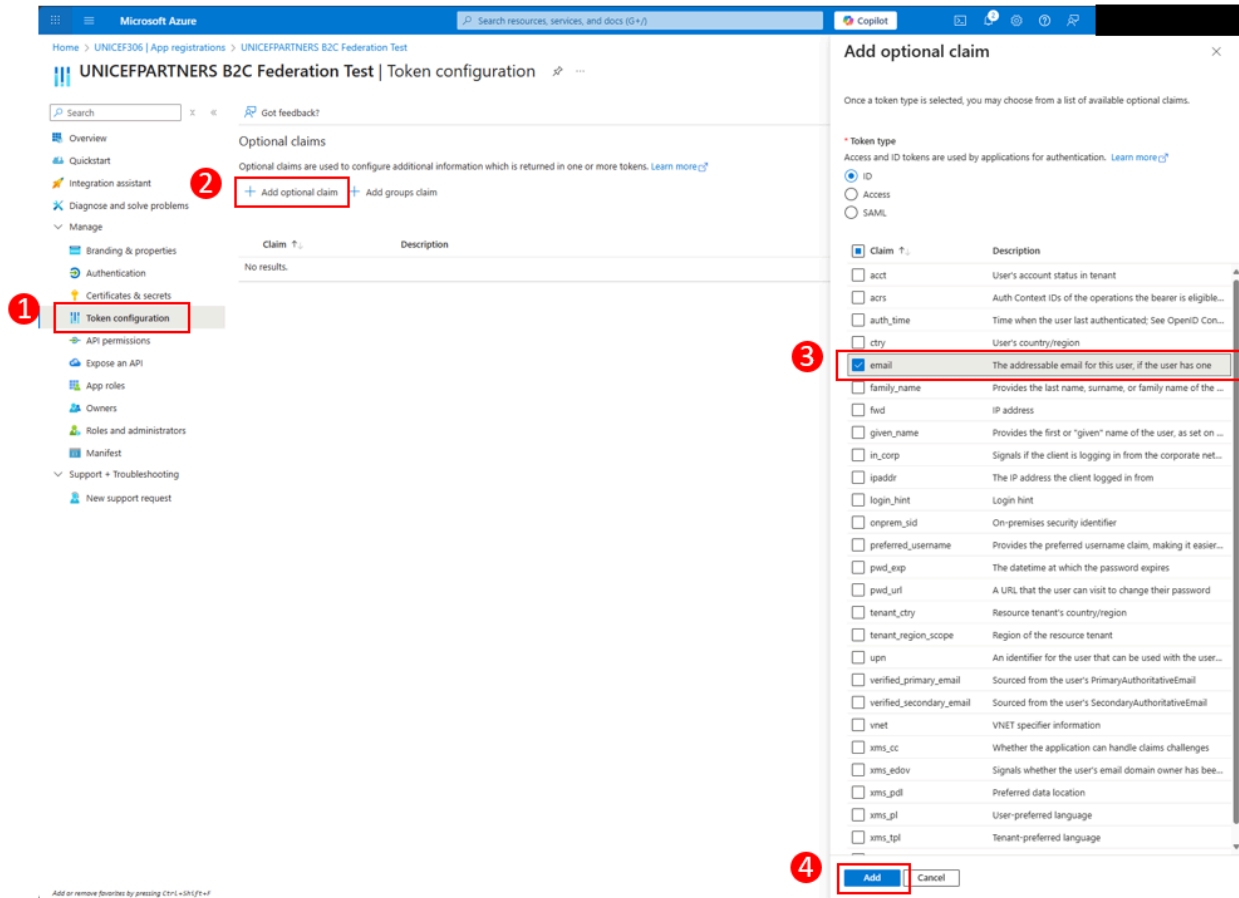
The partner IT focal point must review and complete instructions outlined here: [Set up sign-in for a Microsoft Entra organization - Azure AD B2C | Microsoft Learn](#)

The URL to be used is

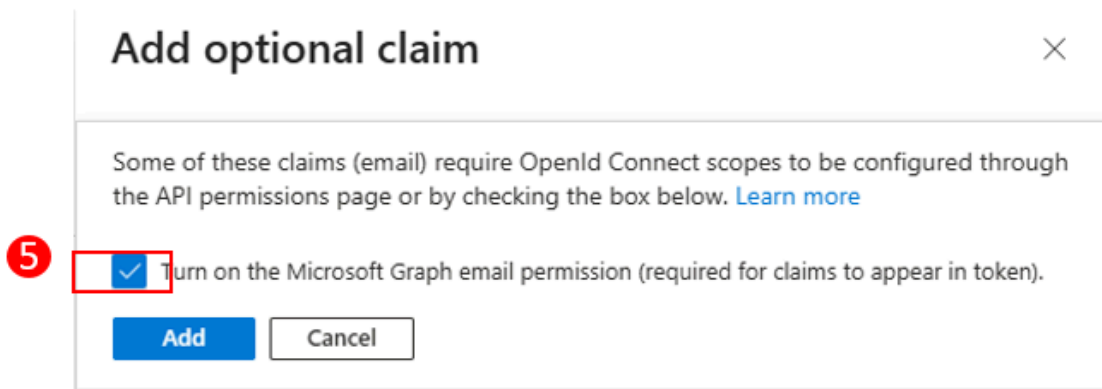
<https://unicefpartners.b2clogin.com/unicefpartners.onmicrosoft.com/oauth2/authresp>

In order to add the email claim into your app registration please follow the below steps:

- 1) Select "Token Configuration"
- 2) Add optional claim
- 3) Select "email"
- 4) Select "Add"



Once you select add, please select “Turn on the Microsoft Graph email permission...”



Once added then:

- 6) Go to “API permissions”
- 7) Select email
- 8) Grant admin consent for your organization

9) Verify email has been granted access

Microsoft Azure

Home > UNICEF306 | App registrations > UNICEFPARTNERS B2C Federation Test

UNICEFPARTNERS B2C Federation Test | API permissions

Search resources, services, and docs (G+)

Copilot

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

New support request

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

Grant admin consent for UNICEF306

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				...
email	Delegated	View users' email address	No	Granted for UNICEF306
User.Read	Delegated	Sign in and read user profile	No	Granted for UNICEF306

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Step 2:

The partner must share credentials via OneDrive or through a safe data transfer method of their choosing with jpanchalingam@unicef.org only.

Step 3:

UNICEF ICTD will provide a test link. If any issues arise during testing then further debugging will be scheduled over a call with UNICEF ICTD (based in Valencia, Spain)