

Wilma OpenID and Azure AD

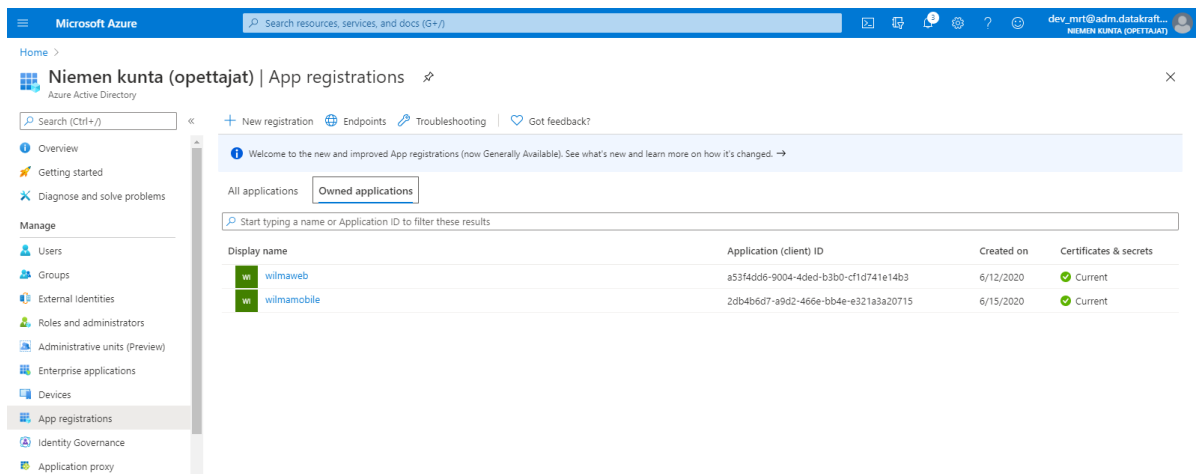
This document describes how to configure Azure AD tenant to support OpenId authentication with Wilma web app and mobile app.

Basic information

To enable OpenId Connect in Azure AD we have register two different apps, one for Wilma web app and one for mobile app.

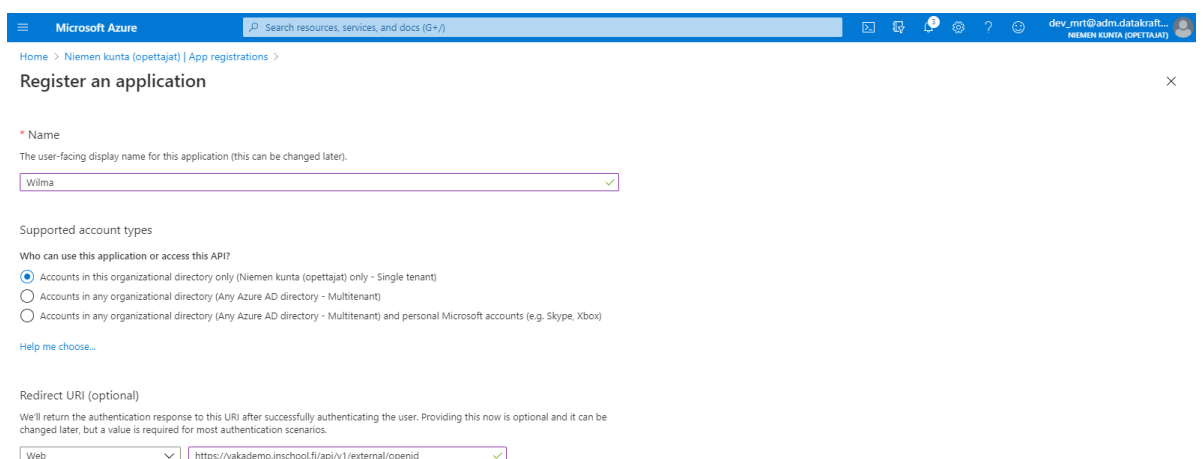
Web app registration

1. Navigate to your tenant and go to *App registrations* and choose *New registration*.



Display name	Application (client) ID	Created on	Certificates & secrets
wilmaweb	a53f4dd6-9004-4ded-b3b0-c1d741e14b3	6/12/2020	Current
wilmamobile	2db4b6d7-89d2-466e-bb4e-e321a3a20715	6/15/2020	Current

2. Fill out the information that fits your situation and hit Register. Redirect URI type must be "Web" and URI should be e.g. "https://testwilma.fi/api/v1/external/openid".

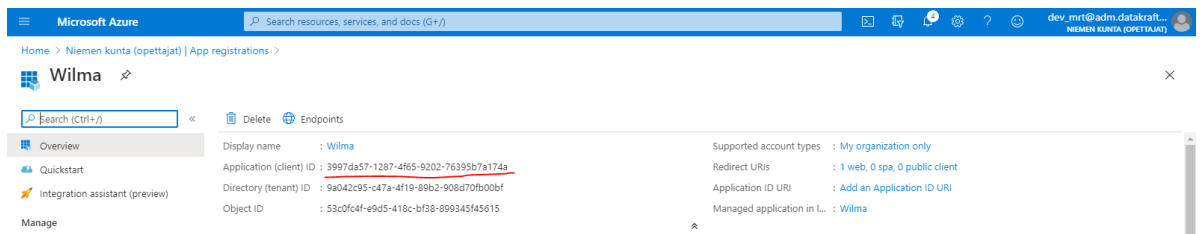


* Name
The user-facing display name for this application (this can be changed later).
Wilma

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Niemen kunta (opettajat) only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
 Web | https://vakademo.inschool.fi/api/v1/external/openid

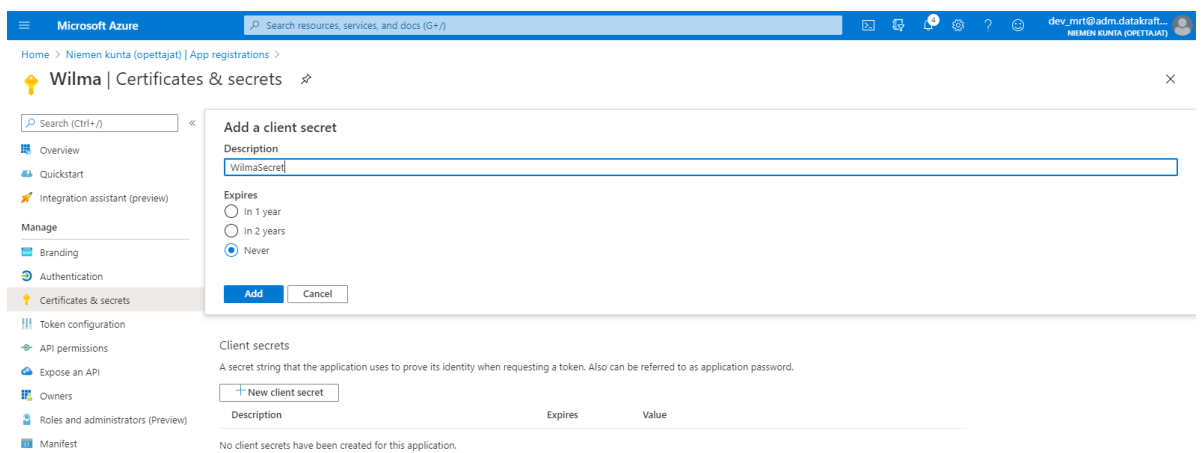
- After registration you will be taken to your App's overview page where you can see the **Client id** automatically assigned to this app.



The screenshot shows the 'Overview' page for the 'Wilma' application in the Microsoft Azure portal. The left sidebar contains navigation options: Overview, Quickstart, Integration assistant (preview), and Manage. The main content area displays the following details:

- Display name: Wilma
- Application (client) ID: 3997da57-1287-4f65-9202-76395b7a174a
- Directory (tenant) ID: 9a042c95-c47a-4f19-89b2-908d70fb00bf
- Object ID: 53c0fc4f-e9d5-418c-bf38-89934545615
- Supported account types: My organization only
- Redirect URIs: 1 web, 0 spa, 0 public client
- Application ID URI: Add an Application ID URI
- Managed application in L...: Wilma

- Go to **Certificates & secrets** page, click **New client secret** and fill out settings to what is appropriate for your organisation and click **Add**. However, if you choose an expiring secret you must remember to create a new secret and update it to Primus when the secret expires.

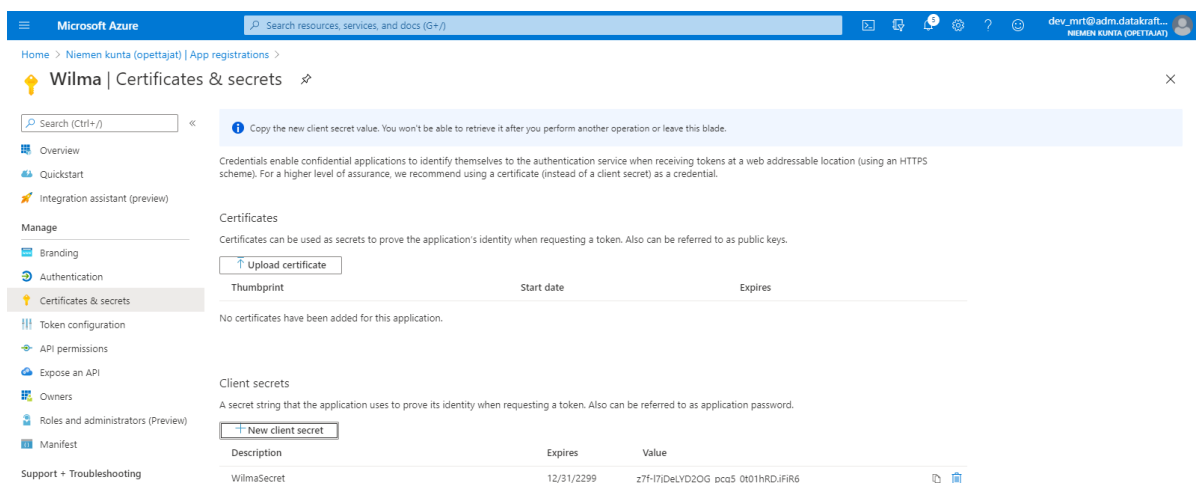


The screenshot shows the 'Certificates & secrets' page for the 'Wilma' application. A modal dialog titled 'Add a client secret' is open, with the following fields and options:

- Description: WilmaSecret
- Expires: In 1 year, In 2 years, Never
- Buttons: Add, Cancel

Below the dialog, the 'Client secrets' section is visible, showing a table with columns for Description, Expires, and Value. A '+ New client secret' button is present above the table.

- Copy the secret and put it somewhere safe. It will not be shown after you leave or refresh the page.

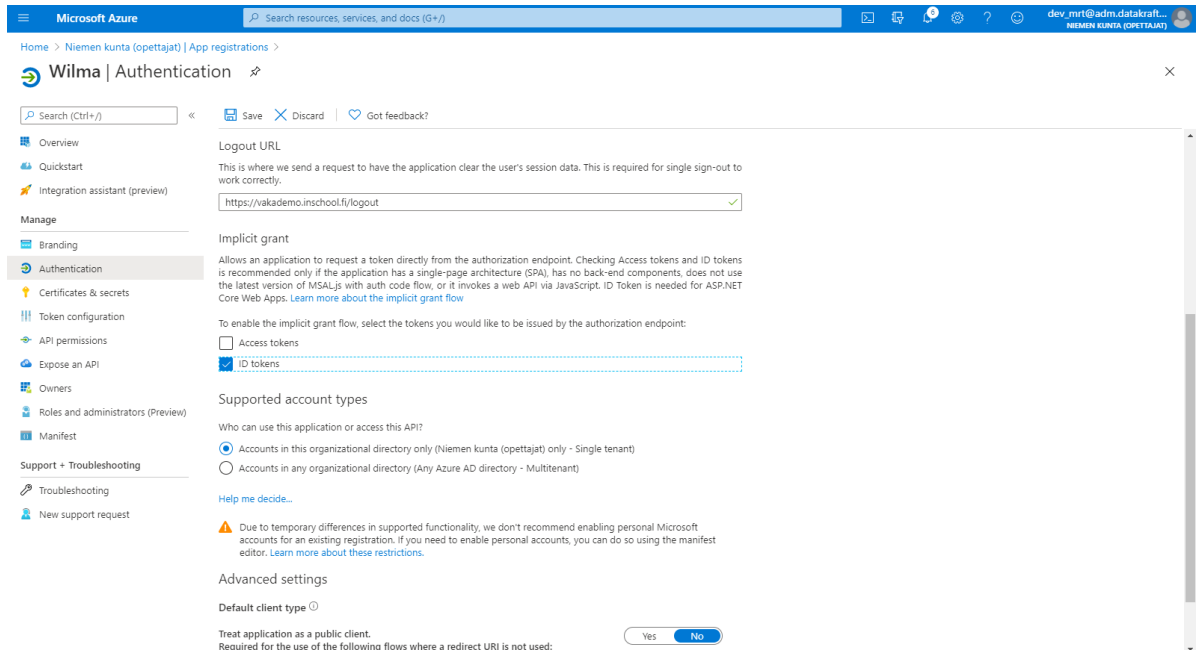


The screenshot shows the 'Certificates & secrets' page after a client secret has been added. A blue notification banner at the top states: 'Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.' Below this, the 'Client secrets' section shows a table with the following data:

Description	Expires	Value
WilmaSecret	12/31/2299	z7f-17jDeLYD2OG_pcg5_0t01HRD.JfIR6

The 'Value' column contains a long alphanumeric string that is partially obscured by a copy icon.

- Go to *Authentication* page and scroll down to **Implicit grant** section. Check *ID Tokens* to enable hybrid flow. Also fill in Logout URL which should be e.g. "https://testwilma.fi/logout" and hit Save.



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

Home > Niemen kunta (opettajat) | App registrations > Wilma | Authentication

Logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

https://vakademo.inschool.fi/logout

Implicit grant

Allows an application to request a token directly from the authorization endpoint. Checking Access tokens and ID tokens is recommended only if the application has a single-page architecture (SPA), has no back-end components, does not use the latest version of MSAL.js with auth code flow, or it invokes a web API via JavaScript. ID Token is needed for ASP.NET Core Web Apps. [Learn more about the implicit grant flow](#)

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

Access tokens

ID tokens

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Niemen kunta (opettajat) only - Single tenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

[Help me decide...](#)

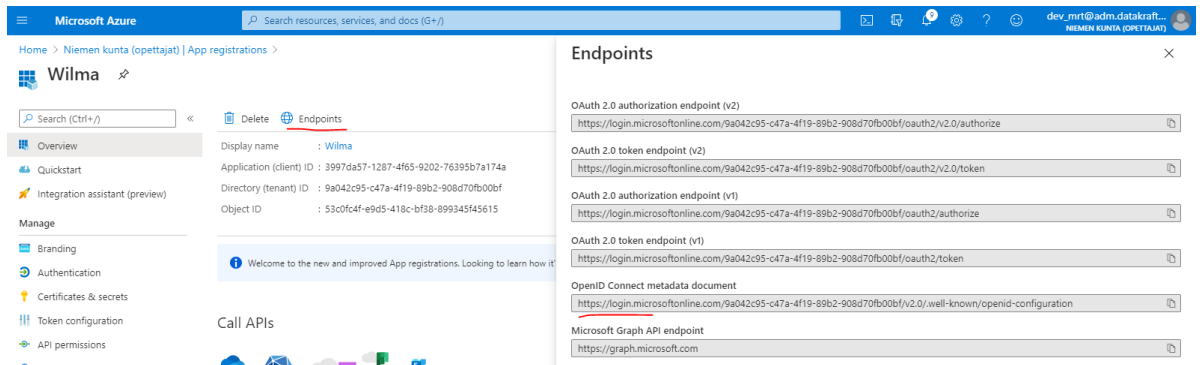
Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Default client type

Treat application as a public client. Required for the use of the following flows where a redirect URI is not used: Yes No

- Head back *Overview* page and click *Endpoints*. Grab the URI in *OpenId Connect Metadata document* and fill this to [Primus OIDC Table](#) along with the **Client ID** and **Client Secret**.



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

Home > Niemen kunta (opettajat) | App registrations > Wilma | Endpoints

Display name : Wilma

Application (client) ID : 3997da57-1287-4f65-9202-76395b7a174a

Directory (tenant) ID : 9a042c95-c47a-4f19-89b2-908d70fb00bf

Object ID : 53c0fc4f-e9d5-418c-bf38-899345f45615

Welcome to the new and improved App registrations. Looking to learn how it works?

Call APIs

Endpoints

OAuth 2.0 authorization endpoint (v2)

https://login.microsoftonline.com/9a042c95-c47a-4f19-89b2-908d70fb00bf/oauth2/v2.0/authorize

OAuth 2.0 token endpoint (v2)

https://login.microsoftonline.com/9a042c95-c47a-4f19-89b2-908d70fb00bf/oauth2/v2.0/token

OAuth 2.0 authorization endpoint (v1)

https://login.microsoftonline.com/9a042c95-c47a-4f19-89b2-908d70fb00bf/oauth2/authorize

OAuth 2.0 token endpoint (v1)

https://login.microsoftonline.com/9a042c95-c47a-4f19-89b2-908d70fb00bf/oauth2/token

OpenID Connect metadata document

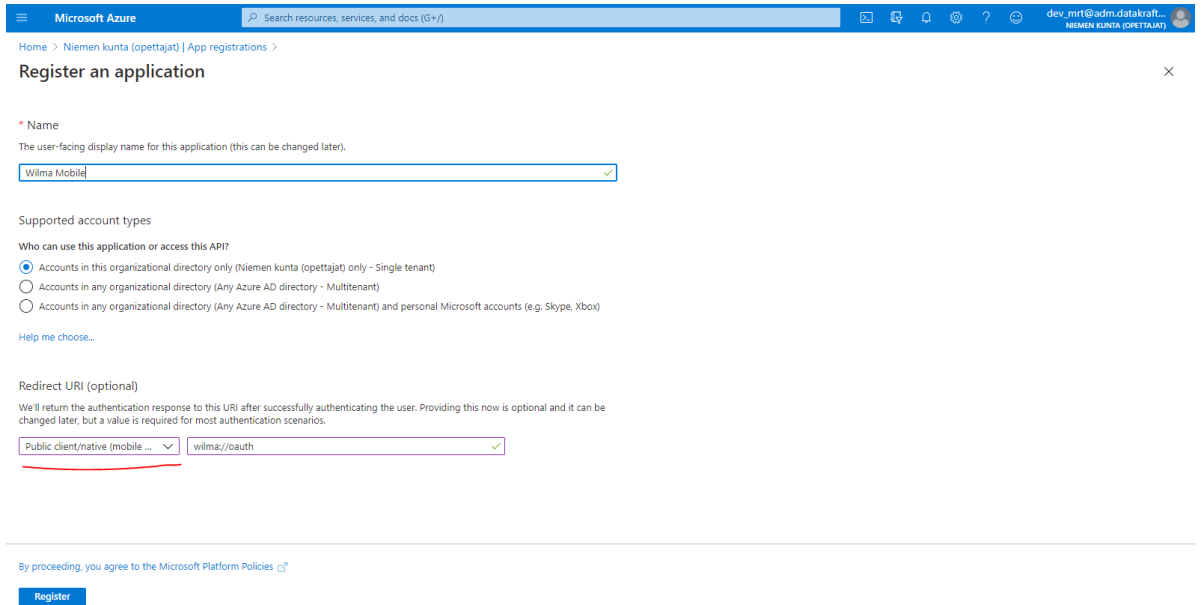
https://login.microsoftonline.com/9a042c95-c47a-4f19-89b2-908d70fb00bf/v2.0/.well-known/openid-configuration

Microsoft Graph API endpoint

https://graph.microsoft.com

Mobile app registration

- Navigate to your tenant and go to *App registrations* and choose *New registration*.
- Fill out the information: Redirect URI type must be "Public client/native" and URI "wilma://oauth". Hit Register.



Microsoft Azure

Home > Niemen kunta (opettajat) | App registrations >

Register an application

Name
The user-facing display name for this application (this can be changed later).

Wilma Mobile

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Niemen kunta (opettajat) only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

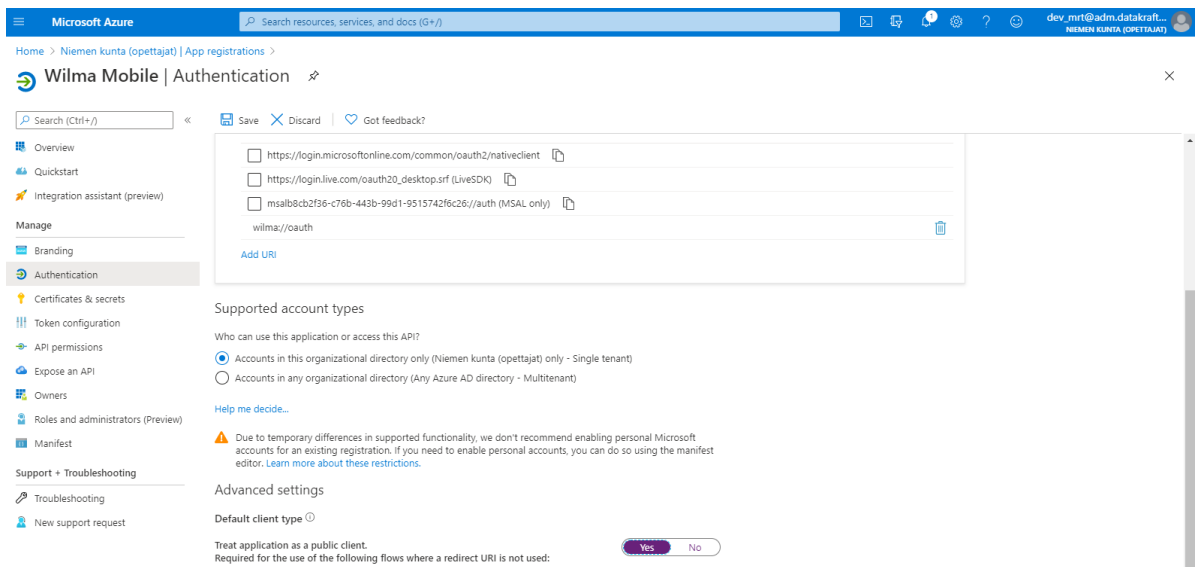
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile ... | wilma://oauth

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

- After registration you will be taken to your App's overview page where you can see the **Client id** automatically assigned to this app.
- Go to **Authentication** page and scroll down to **Advanced settings** section. Set **Treat application as a public client** to Yes and hit Save.



Microsoft Azure

Home > Niemen kunta (opettajat) | App registrations >

Wilma Mobile | Authentication

Overview | Quickstart | Integration assistant (preview) | Manage | Authentication | Certificates & secrets | Token configuration | API permissions | Expose an API | Owners | Roles and administrators (Preview) | Manifest | Support + Troubleshooting | Troubleshooting | New support request

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Niemen kunta (opettajat) only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)

[Help me decide...](#)

Advanced settings

Default client type

Treat application as a public client. Required for the use of the following flows where a redirect URI is not used: **Yes** No

- Head back **Overview** page and click **Endpoints**. Grap the URI in **OpenId Connect Metadata document** and fill this to [Primus OIDC Table](#) along with the **Client ID**.