Wilma OpenID and Azure AD

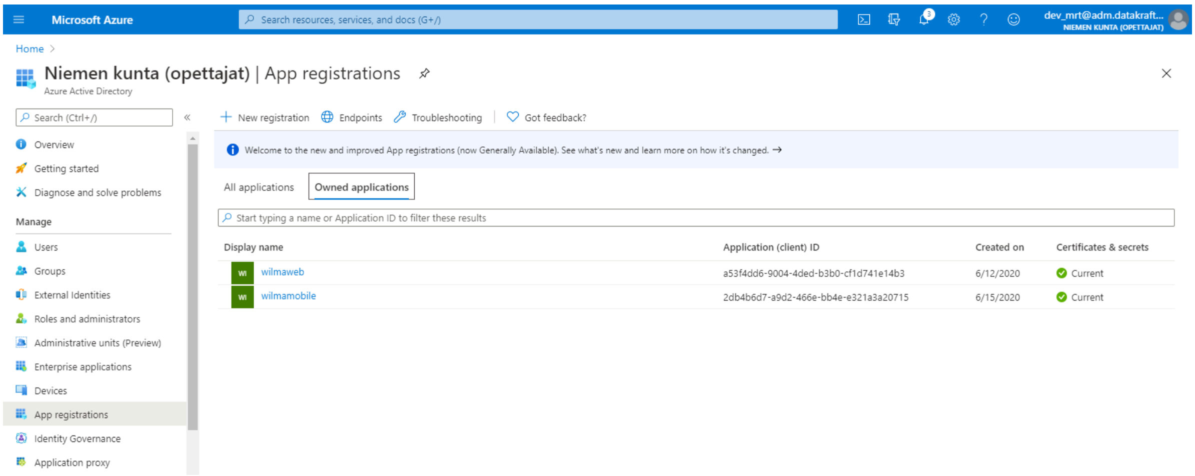
This document describes how to configure Azure AD tenant to support OpenId authentication with Wilma web app and mobile app.

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.*



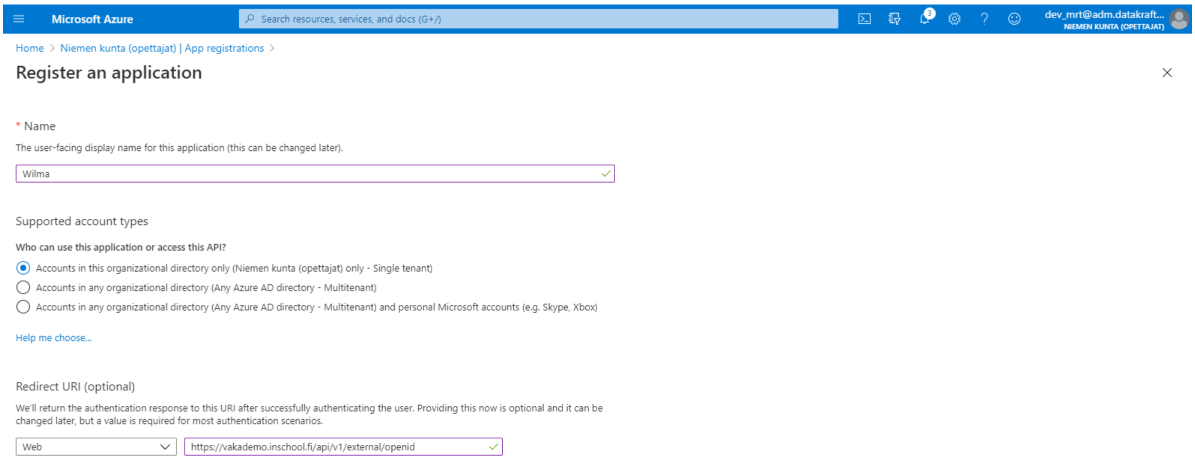
Niemen kunta (opettajat) | App registrations

Azure Active Directory

Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →

Display name	Application (client) ID	Created on	Certificates & secrets
WI wilmaweb	a53f4dd6-9004-4ded-b3b0-cf1d741e14b3	6/12/2020	✓ Current
WI wilmamobile	2db4b6d7-a9d2-466e-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".


Microsoft Azure
Search resources, services, and docs (G+/)
dev_mrt@adm.datakraft...
NIEMEN KUNTA (OPETTAJAT)
Home > Niemen kunta (opettajat) | App registrations >
Help me choose...

Register an application

* 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?

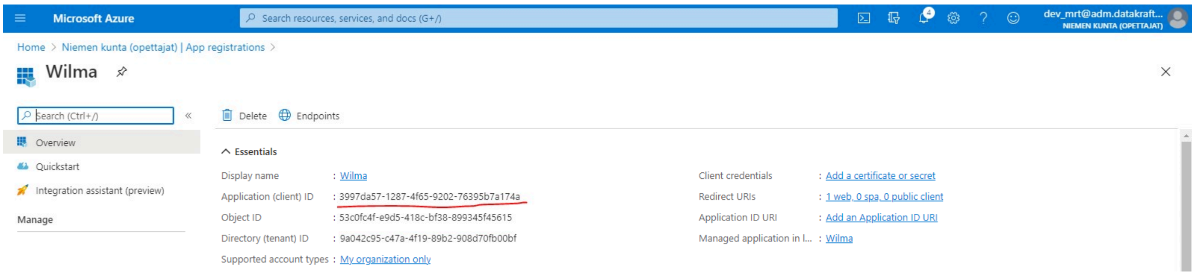
● Accounts in this organizational directory only (Niemen kunta (opettajat) only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype,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

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.

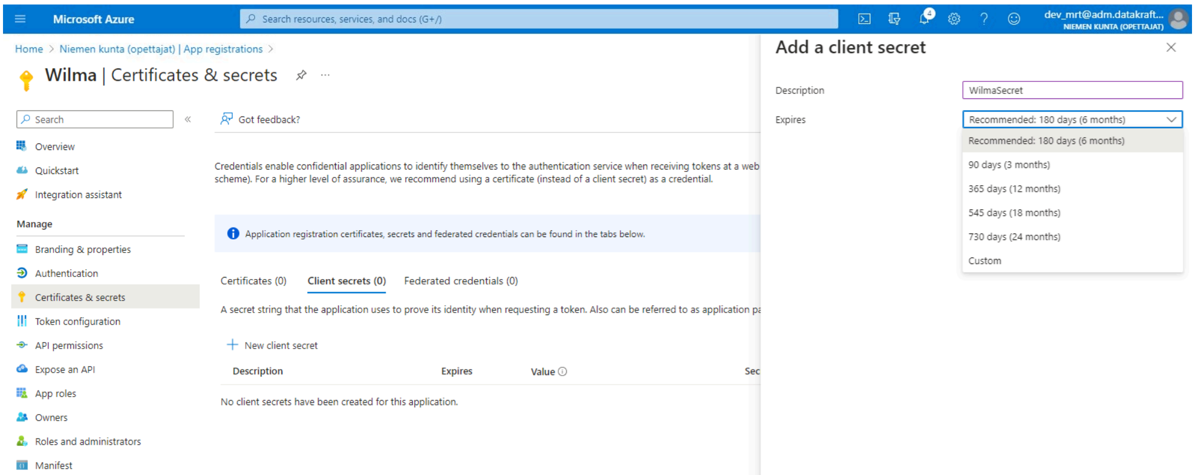
Web | https://vakademo.inschool.fi/api/v1/external/openid ✓

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



Display name : Wilma
Application (client) ID : 3997da57-1287-4f65-9202-76395b7a174a
Object ID : 53c0fc4f-e9d5-418c-bf38-899345f45615
Directory (tenant) ID : 9a042c95-c47a-4f19-89b2-908d70fb00bf
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : 1 web, 0 spa, 0 public client
Application ID URI : Add an Application ID URI
Managed application in l... : Wilma

4. Go to *Certificates & secrets* page, click *New client secret* and fill out settings to what is appropriate for your organisation and click *Add*. You must remember to create a new secret and update it to Primus when the secret expires.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

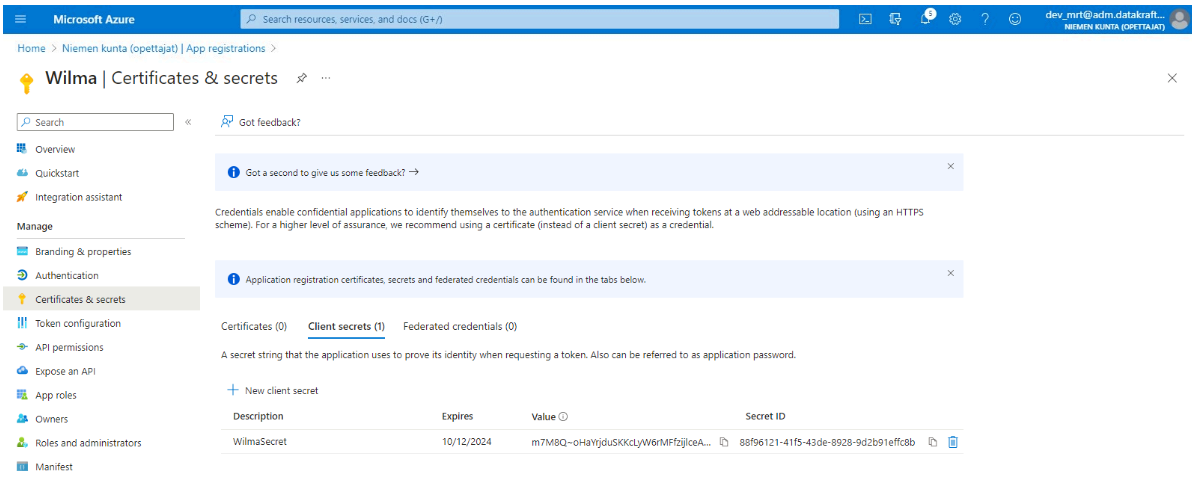
Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application pa

No client secrets have been created for this application.

Description: WilmaSecret
Expires: Recommended: 180 days (6 months)

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



Got a second to give us some feedback? →

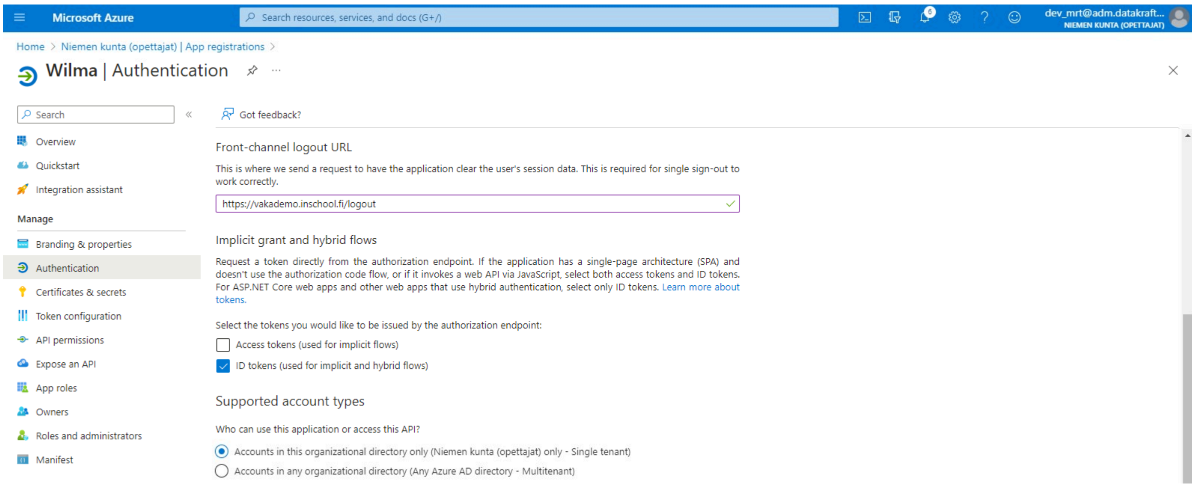
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
WilmaSecret	10/12/2024	m7M8Q~oHaYrjduSKKcLyW6rMFfzijlceA...	88f96121-41f5-43de-8928-9d2b91effc8b

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



Wilma | Authentication

Front-channel 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 and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

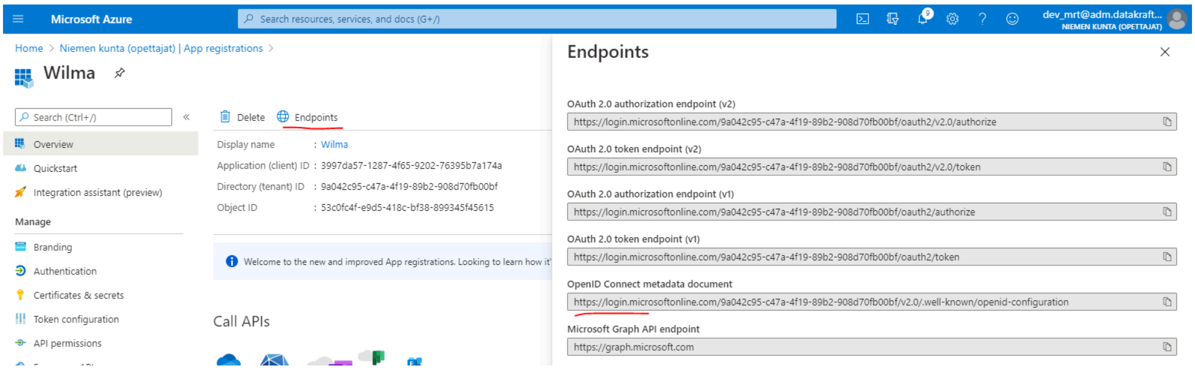
Supported account types

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)

7. 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** and **Client Secret**.



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'

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

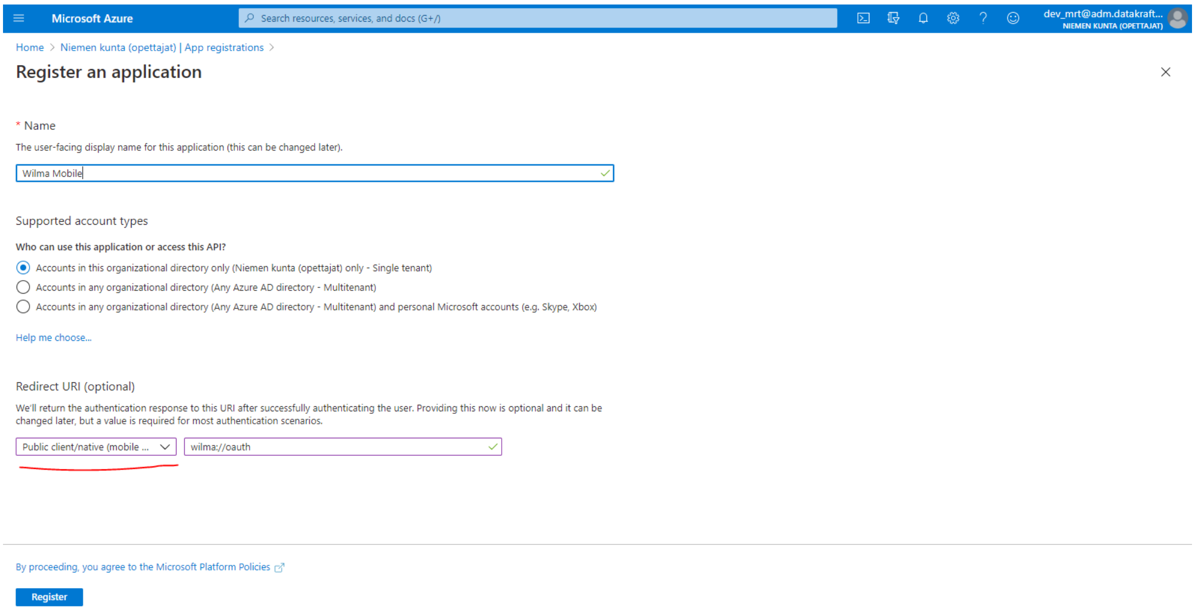
OpenID Connect metadata document
https://login.microsoftonline.com/9a042c95-c47a-4f19-89b2-908d70fb00bf/v2.0/.well-known/openid-configuration

Microsoft Graph API endpoint
https://graph.microsoft.com

Mobile app registration

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

2. Fill out the information: Redirect URI type must be "Public client/native" and URI "wilma://oauth". Hit Register.



Microsoft Azure
Search resources, services, and docs (G+/)
dev_mrt@adm.datakraft...
NIEMEN KUNTA (OPETTAJAT)
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)

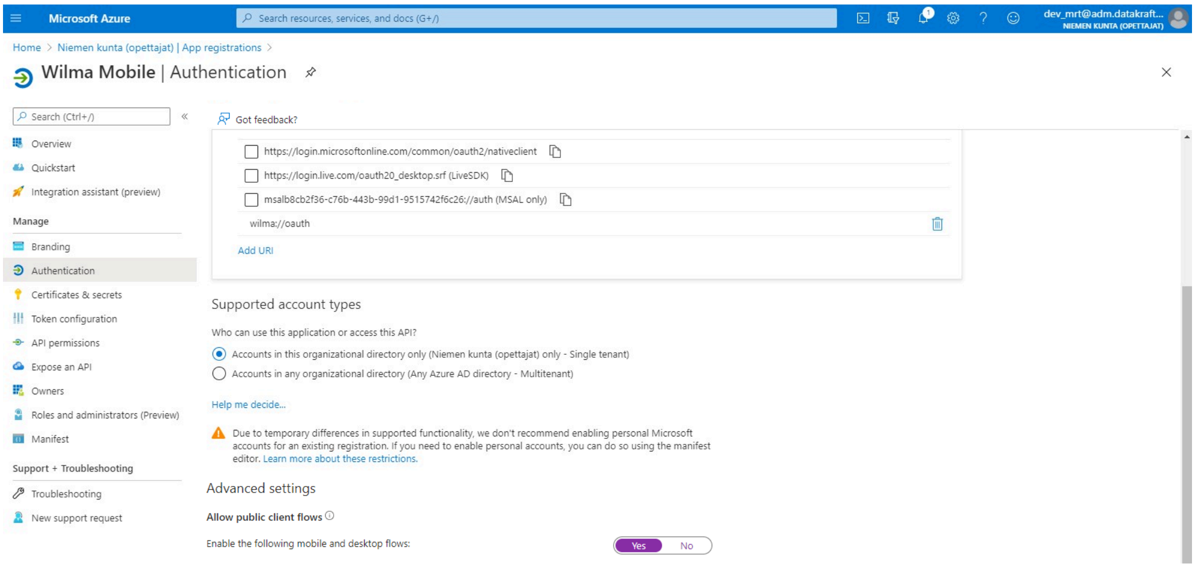
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

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

By proceeding, you agree to the Microsoft Platform Policies

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

4. Go to *Authentication* page and scroll down to **Advanced settings** section. Set *Enable the following mobile and desktop flows* to *Yes* and hit *Save*.



Wilma Mobile | Authentication

□ https://login.microsoftonline.com/common/oauth2/nativeclient

□ https://login.live.com/oauth20_desktop.srf (LiveSDK)

□ msalb8cb2f36-c76b-443b-99d1-9515742f6c26://auth (MSAL only)

wilma://oauth

Add URI

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

Allow public client flows

Enable the following mobile and desktop flows: [✓ Yes] No

5. 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**.