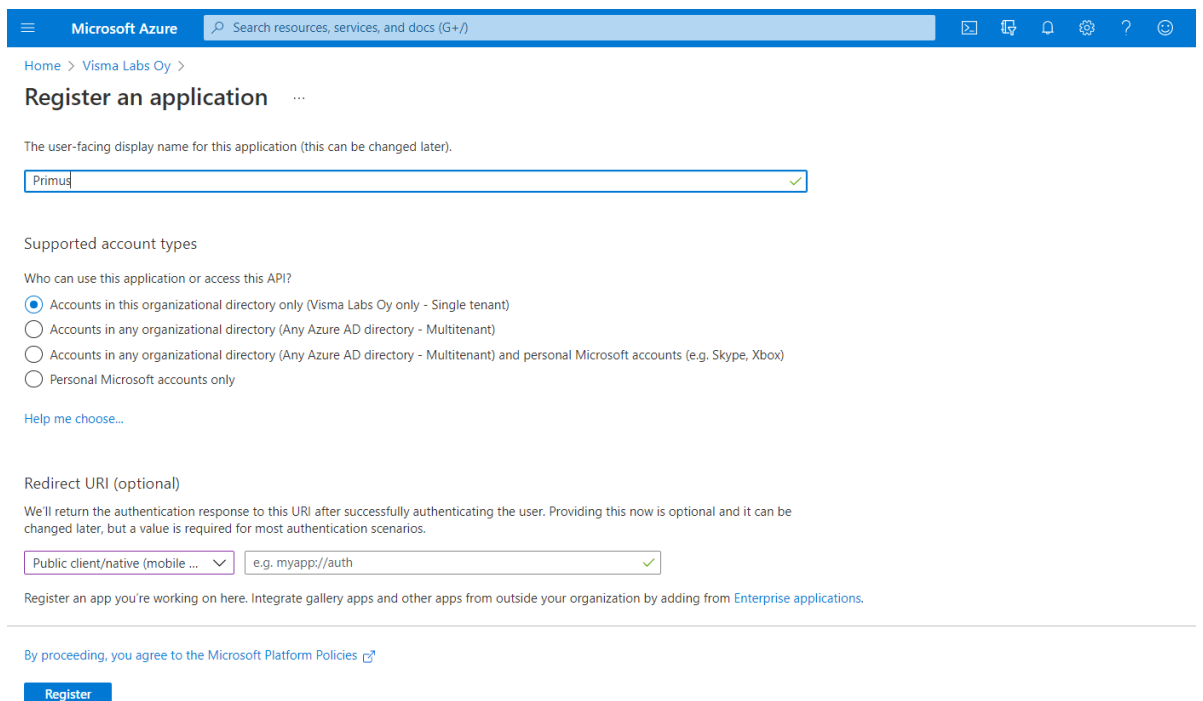


Primus OpenID and Azure AD

This document describes how to configure Azure AD tenant to support OpenID authentication with Primus client.

Primus client application 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". URI should be left as it is. Hit Register.



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

Home > Visma Labs Oy >

Register an application

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

Primus

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Visma Labs Oy 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)

Personal Microsoft accounts only

[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.

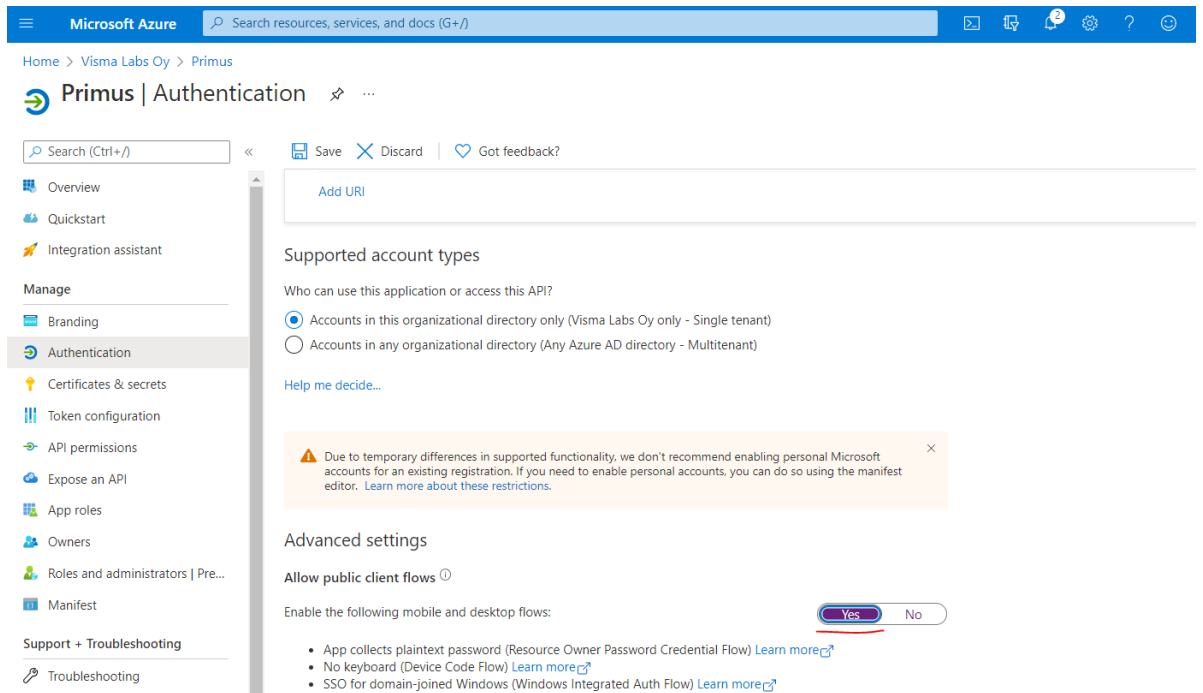
Public client/native (mobile ... e.g. myapp//auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

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

Register

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. On the *Authentication* page and scroll down to **Advanced settings** section. Set *Treat application as public client* to Yes and hit Save.



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure' and a search bar. The breadcrumb trail is 'Home > Visma Labs Oy > Primus'. The main heading is 'Primus | Authentication'. A left-hand navigation pane lists various settings categories: Overview, Quickstart, Integration assistant, Manage (Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators | Pre..., Manifest), and Support + Troubleshooting (Troubleshooting). The 'Authentication' section is selected and expanded, showing an 'Add URI' input field. Below this, the 'Supported account types' section is visible, with the option 'Accounts in this organizational directory only (Visma Labs Oy only - Single tenant)' selected. A warning message states: '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.' The 'Advanced settings' section includes a toggle for 'Allow public client flows' which is currently set to 'Yes'. Below this, there are three bullet points with links to learn more: 'App collects plaintext password (Resource Owner Password Credential Flow)', 'No keyboard (Device Code Flow)', and 'SSO for domain-joined Windows (Windows Integrated Auth Flow)'.

- 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**.
 OIDC Flow type should be set to *Device code*.