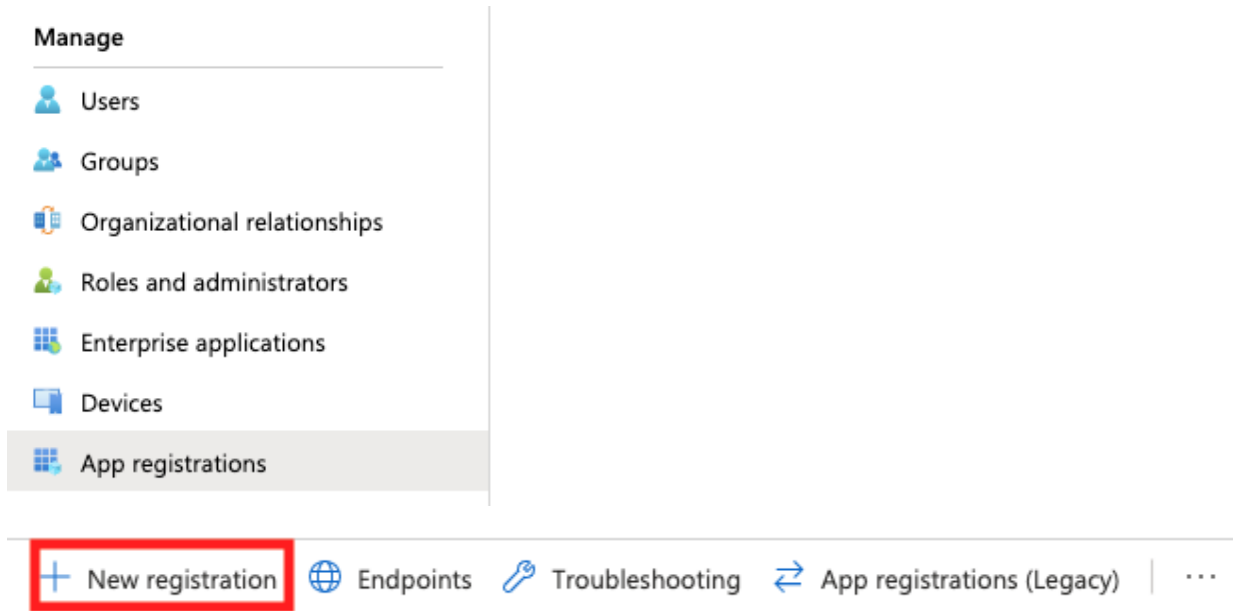


Azure AD -integraatio

Tässä dokumentissa kuvataan lyhyesti MPASSid palvelun käyttöönottaminen AzureAD integraatiota hyödyntäen. Ennakkovaatimuksena integraatiolle on että MPASSid tietomallin mukaiset tiedot ovat luettavissa käyttäjähakemistosta. Lisätietoja tietosisällöllisistä vaatimuksista löytyy täältä: <https://wiki.eduuni.fi/jat9bq>

AzureAD:n konfigurointi

1. Microsoft Azure portaalissa valitse "App registrations" ja "New registration"



The screenshot shows the Azure AD portal navigation menu on the left, with 'App registrations' highlighted. Below the menu is a horizontal navigation bar with several options: '+ New registration' (highlighted with a red box), 'Endpoints', 'Troubleshooting', 'App registrations (Legacy)', and a menu icon. The 'New registration' button is a blue square with a white plus sign and the text 'New registration'.

Register an application

* Name

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

MPASSid ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory 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://mpass-proxy.csc.fi/Shibboleth.sso/SAML2/POST>

2. Lisää kohtaan "Add an Application ID URI":

Display name	: MPASSid	Supported account types	: My organization only
Application (client) ID	: 12345678901234567890123456789012	Redirect URIs	: 1 web, 0 public client
Directory (tenant) ID	: 98765432109876543210987654321098	Application ID URI	: Add an Application ID URI
Object ID	: 54321098765432109876543210987654	Managed application in ...	: MPASSid

Application ID URI  **Set**

Scopes defined by this API

Define custom scopes to restrict access to data
API can request that a user or admin consent to

Klikkaa Set ja aseta siihen: <https://mpass-proxy.csc.fi/shibboleth>

3. Anna tarvittavat käyttöoikeudet Azure AD:hen. Valitse vasemmasta valikosta "API permissions" ja sen jälkeen "Add a permission"

Valitse Microsoft Graph

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs



Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Delegated permissions

- Directory / Directory.AccessAsUser.All (Access directory as the signed in user)
- Directory / Directory.Read.All (Read directory data)
- Oletuksena pitäisi olla jo: User.Read (Sign in and read user profile)

Application permissions

- Directory / Directory.Read.All (Read directory data)

Hyväksy muutokset painamalla: "Grant admin consent for ...".

4. MPASSid sovellus tarvitsee salasanan päästäkseen integroitumaan AzureAD:n kanssa

Valitse vasemmalta "Certificates & secrets"

Client secrets

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
-------------	---------	-------

No client secrets have been created for this application.

Luo uusi client secret.

Anna avaimelle nimi ja valitse kesto (mieluiten expires never). Valitse Add ja muista kopioida avain tässä kohtaa talteen, koska et enää pääse näkemään sitä suljettuasi sivun.

5. MPASSid tiimi tarvitsee seuraavat tiedot asennuksen viimeistelemiseksi

- Application (client) ID
- Directory (tenant) ID
- Client secret (avain)
- Tiedon mistä Azure AD:n attribuuteista MPASSid:lle välitettävät käyttäjätiedot löytyvät ([Yleiset vaatimukset](#)).