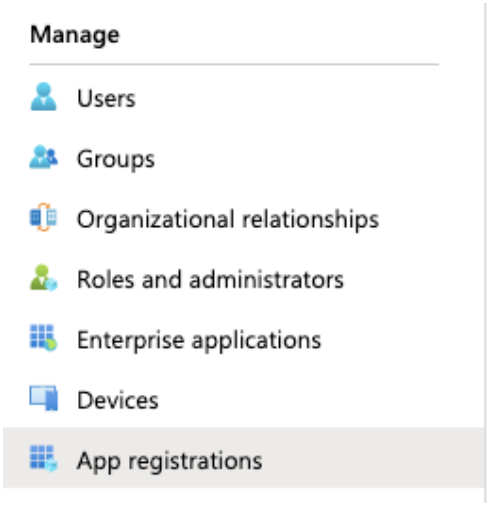
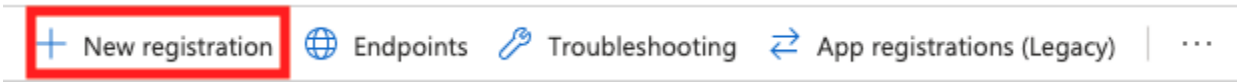
Azure AD -integraatio

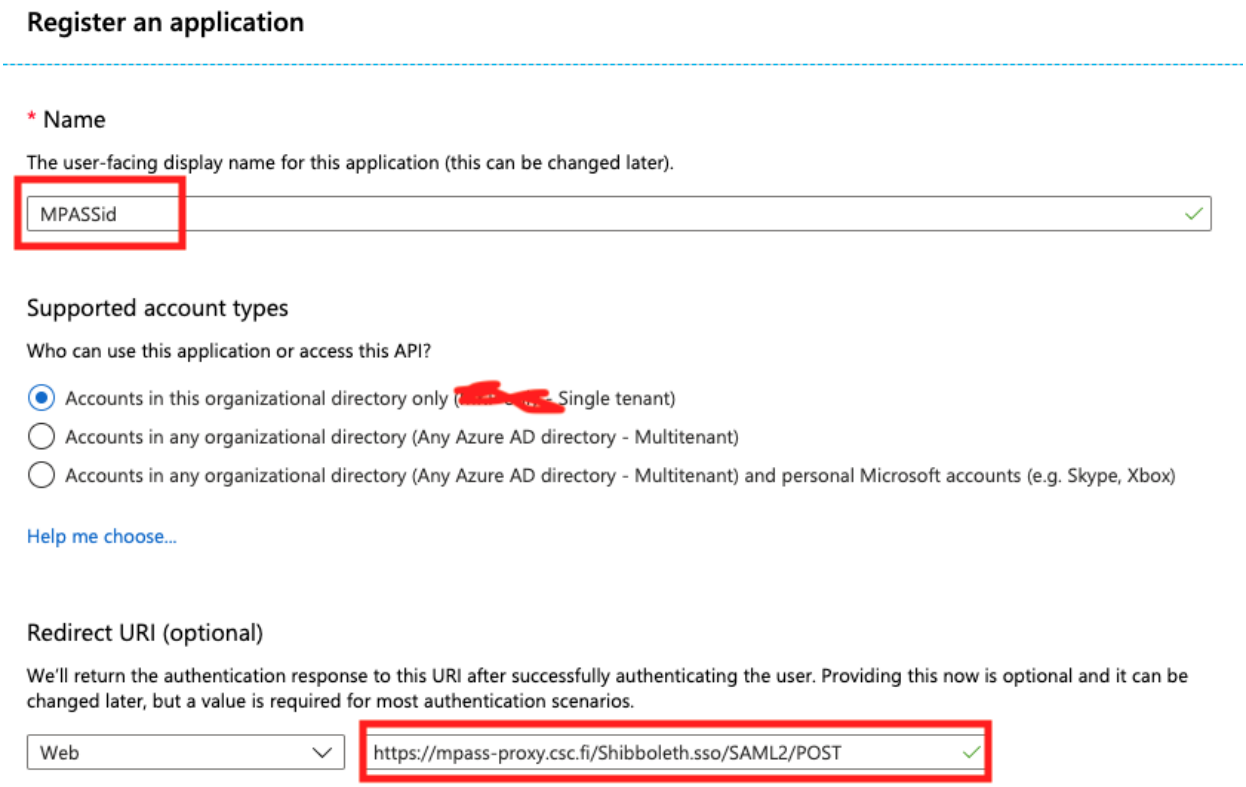
Tässä dokumentissa kuvataan lyhyesti MPASSid palvelun käyttöönottaminen AzureAD integraatiota hyödyntäen. Ennakkovaatimuksena integraatiolle on että MPASSid tietomallin mukaiset tiedot ovat luettavissa käyttäjähakemistosta. Lisätietoja tietosisällöllisistä vaatimuksista löytyy täältä: https://wiki.eduuni.fi/x/JAT9BQ

AzureAD:n konfigurointi

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

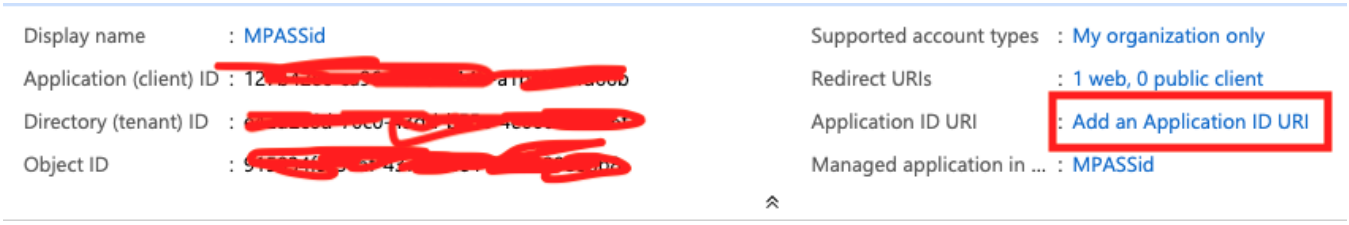


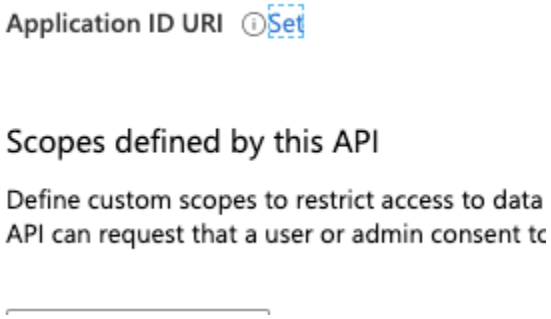




https://mpass-proxy.csc.fi/Shibboleth.sso/SAML2/POST

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

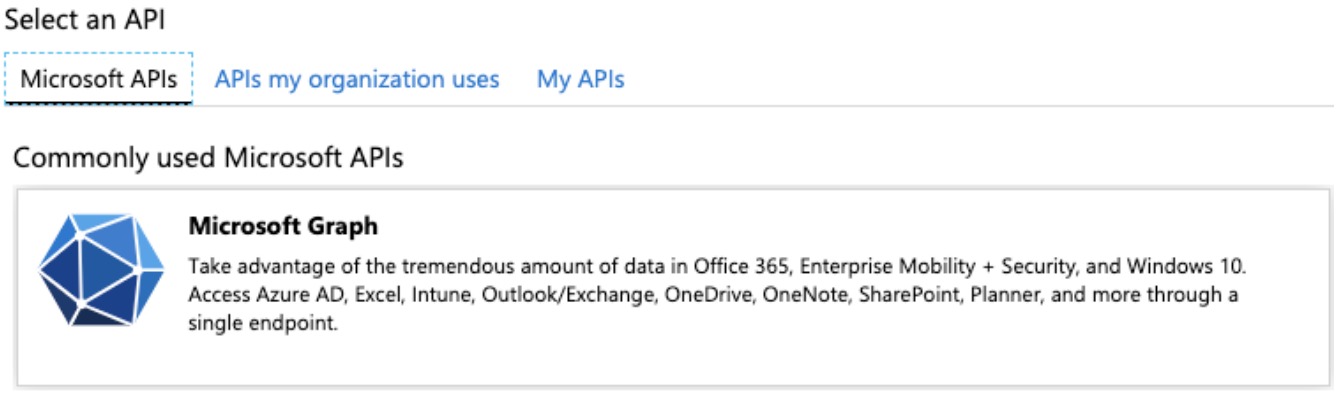




Klikkaa Set ja aseta siihen: https://mpass-proxy.csc.fi/shibboleth

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

Valitse Microsoft Graph



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)

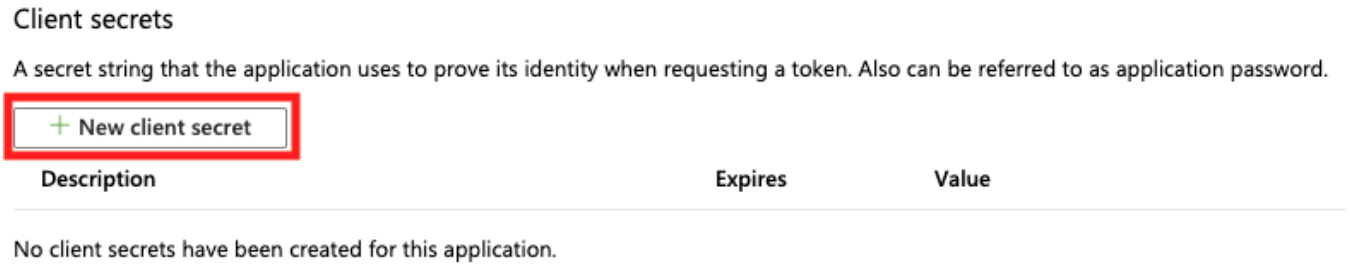
Application permissions

- 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"



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).