

Azure AD (Entra ID) -integraatio

Tässä dokumentissa kuvataan MPASSid palvelun käyttöönottona Azure AD -integraatiota hyödyntäen. Ennakkovaatimuksena integraatiolle on että MPASSid tietomallin mukaiset tiedot ovat luettavissa käyttäjähakemistosta. Lisätietoja tietosisällöllisistä vaatimuksista löytyy täältä: <https://wiki.eduuni.fi/x/8rMID>

App registration luonti

MPASSid tarvitsee Azure AD tenantiinne App registration sovelluksen, jonka kautta käyttäjän attribuutit noudetaan kirjautumisen yhteydessä. Alla olevien ohjeiden avulla voit luoda Azure AD tenantiisi MPASSid:n tarvitseman App registration:n tarvittavilla asetuksilla. App registration:n luodaan joko GUIn tai PowerShellin kautta, voit itse valita kumpaa tapaa käyttää.

Suosittelme myös tutustumaan jo etukäteen Client secret vaihtoprosessiin.

- [App registration - PowerShell](#)
- [App registration - GUI](#)
- [Azure AD app registration client secret -vaihtoprosessi](#)

Lista vaadittavista tiedoista

Selite	Azure AD attribuutti (Graph API:n tarjoama kirjoitusasu)	Pakollinen	Huomioita
Huom! attribuutteihin saattaa tulla muutoksia, huomioi voimassaoleva tietomalli			
Sukunimi		x	
Etunimi		x	
Kutsumanimi			Tietomallissa 1.4 alkaen
Koulukoodi		x	
Luokka tai ryhmä		(x)	Pakollinen perusasteen oppilaille.
Luokka-aste		(x)	Pakollinen perusasteen oppilaille.
Rooli		x	
Kansallinen oppijanumero		x	
Oppimateriaalien maksullisuus		(x)	Pakollinen toisen asteen opiskelijoille.
Muut pakolliset tiedot			
Directory (tenant) ID		x	
Application (client) ID		x	
Client secret (Value EI Secret ID)		x	Tämä tulee lähettää turvapostilla. Toimita myös avaimen voimassaolon päättymisajankohta
Application ID URI		x	Muoto: (api://<guid>)
Oppilaitostyytit		x - jos uusi integraatio	
Logo		x - jos uusi integraatio	125x36px png-muodossa
Koulutuksenjärjestäjän OID		x - jos uusi integraatio	
Redirect URI			OPH toimittaa tämän koulutuksenjärjestäjälle

Huom! attribuuttien nimet eivät Azure AD:n graafisessa hallintaliittymässä vastaa Graph API:n kautta haettavia nimiä. Voit tarkistaa attribuuttien oikeellisuuden [Microsoftin API-dokumentaation](#) avulla, tai tämän sivun lopusta löytyvällä PowerShell funtiolla. Voit myös hyödyntää tämän sivun lopun "Esimerkki funktion käytöstä" optionalAttributes -listaa, jossa on listattu iso osa MPASSid:n muissa Azure AD integraatioissa käytössä olevia attribuutteja.

Azure AD attribuuttien nimien varmistaminen

Azure AD:ssa attribuuttien tekniset nimet saattavat poiketa graafisen käyttöliittymän nimistä. MPASSid hakee tiedot Microsoft Graph API:n kautta. Sitä kautta noudettaessa tulee tietää attribuuttien tekniset nimet ja attribuuttien kirjainkoonkin tulee olla oikein (surname vs Surname).

Alla olevan powershell funktion avulla voi varmistaa attribuuttien kirjoitusasun hakemalla esimerkiksi jonkin Azure AD:ssa olevan testitunnuksen tiedot. Onkin suositeltavaa testata ensin sen avulla attribuuttien oikea kirjoitusasu.

Funktio copy-pastetaan powershell ikkunaan ja sen jälkeen sitä kutsutaan getAccountAttributes -komennolla samassa ikkunassa.

```
function getAccountAttributes {
    param (
        [Parameter()]
        [string] $clientId,
        [Parameter()]
        [string] $clientSecret,
        [Parameter()]
        [string] $tenantId,
        [Parameter()]
        [string] $userPrincipalName,
        [Parameter()]
        [string] $optionalAttributes
    )

    $ReqTokenBody = @{
        Grant_Type = "client_credentials"
        Scope      = "https://graph.microsoft.com/.default"
        client_Id  = $clientId
        Client_Secret = $clientSecret
    }

    $TokenResponse = Invoke-RestMethod -Uri "https://login.microsoftonline.com/$tenantId/oauth2/v2.0/token" -
Method POST -Body $ReqTokenBody

    if ( !$optionalAttributes )
    {
        $apiUrl = "https://graph.microsoft.com/v1.0/users/" + $userPrincipalName
    } else {
        $apiUrl = "https://graph.microsoft.com/v1.0/users/" + $userPrincipalName + "?`$select=displayName,
givenName,surname,userPrincipalName,id,$optionalAttributes "
    }

    $Data = Invoke-RestMethod -Headers @{Authorization = "Bearer $($TokenResponse.access_token)" } -Uri $apiUrl -
Method Get

    return ( $data )
}
```

```
# Esimerkki funktion käytöstä.
# Ilman -optionalAttributes parametria komento hakee käyttäjäobjektin perustiedot (näyttönimi, etunimi,
sukunimi ja UPN).
# Voit lisätä -optionalAttributes parametriin lisää attribuuttien nimiä pilkulla eroteltuina.
# Vaihda x, y, ja z arvoiksi yllä luomasi App registration:n ja Azure AD tenantin tiedot.

getAccountAttributes -clientId "xxxxxxxxxxxxxxxxxxxxxxx" -clientSecret "yyyyyyyyyyyyyyyyyy" -tenantId
"zzzzzzzzzzzzzzzzzzzz" -userPrincipalName "<haettavatunnus@domain.onmicrosoft.com>" -optionalAttributes "city,
companyName,department,department,faxNumber,jobTitle,officeLocation,onpremisesextensionattributes,postalCode,
state,streetAddress"
```

OPH:lle toimitettavat tiedot integraatiotyypistä riippumatta

MPASSid-integraation rakentamista varten jokaisen koulutustoimijan on ilmoitettava seuraavat tiedot palveluosoitteeseemme **mpass(at)oph.fi** .

1. Oppilaitostyytit, joilla aiotte MPASSid:tä käyttää. Hyväksytyt oppilaitostyytit koodiarvoineen löytyvät täältä: <https://koski.opintopolku.fi/koski/dokumentaatio/koodisto/oppilaitostyyppi/latest>
2. Kunnan/koulutustoimijan logotiedoston, jonka haluatte näyttävän MPASSid:n koulunvalintasivulla.
 - Logo: png-muodossa, koko 125x36 px.

Kun nämä tiedot on lähetetty MPASSid:lle ja liittymissopimukset ovat allekirjoitettuna molempien osapuolten toimesta, saadaan integraatio päälle usein parin arkipäivän kuluessa.