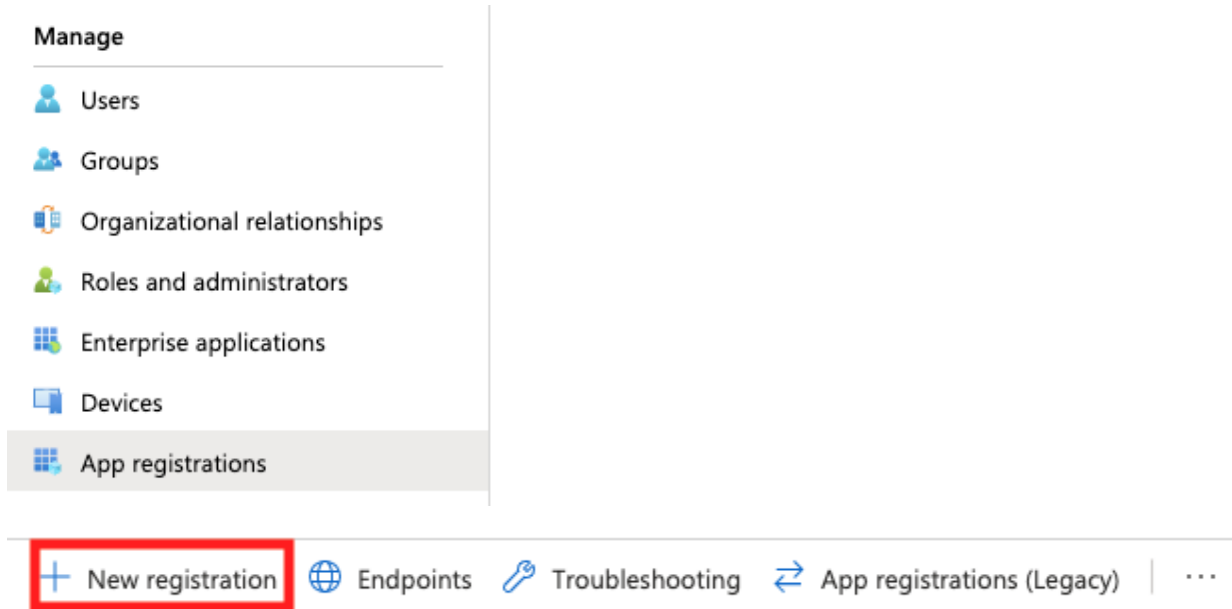


Azure AD-integration

I detta dokument beskrivs kortfattat ibruktagandet av MPASSid-tjänsten med hjälp av AzureAD-integrationen. Ett förhandskrav för integrationen är att uppgifterna enligt MPASSid-datamodellen kan läsas i användarindexet. Mer information om datainnehållskraven finns här: <https://wiki.eduuni.fi/x/8rMID>

Konfiguration av AzureAD

1. Gå till Microsoft Azure-portalen och välj "App registrations" och "New registration"



The screenshot shows the Microsoft Azure portal interface. On the left, the 'Manage' sidebar lists various options: Users, Groups, Organizational relationships, Roles and administrators, Enterprise applications, Devices, and App registrations. The 'App registrations' option is highlighted. On the right, the 'New registration' button is highlighted with a red box. Other buttons visible include Endpoints, Troubleshooting, App registrations (Legacy), and a menu icon.

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>

1. Lägg till URI under "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	: 87654321098765432109876543210987	Application ID URI	: Add an Application ID URI
Object ID	: 98765432109876543210987654321098	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

Klicka på Set och ange: "api://<guid>" värden. Klicka Save

3. Ge erforderliga behörigheter till Azure AD. Välj "API Permissions" i menyn till vänster och därefter "Add a permission".

Välj 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)
- Antaget värdet skulle vara: User.Read (Sign in and read user profile)

Application permissions

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

Godkänn ändringarna genom att klicka på: "Grant admin consent for ..."

4. MPASSid-tillämpningen behöver ett lösenord för integrationen med AzureAD

Välj "Certificates & secrets" till vänster

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.

+ New client secret

Description	Expires	Value
-------------	---------	-------

No client secrets have been created for this application.

Skapa en ny client secret.

Ge nyckeln ett namn och välj önskad giltighetstid för nyckeln. Välj Add och kom ihåg att kopiera nyckeln här eftersom du inte längre kan se den när du stänger sidan.

Obs! Anteckna nyckelns giltighetstid, eftersom inloggningarna i MPASSid slutar fungera om nyckeln inte förnyas hos Azure AD och MPASSid innan den går ut. En ny client secret måste lämnas till MPASSid senast en vecka innan den gamla går ut.

5. MPASSid-teamet behöver följande information för att slutföra installationen

- Application (client) ID
- Directory (tenant) ID
- Client secret (nyckel) och datumet när nyckelns giltighetstid upphör
- Uppgift om i vilka attribut i Azure AD de användaruppgifter som ska förmedlas till MPASSid finns
 - [Se Testning av integrationen](#)

6. Kontroll av namnen på attributen i Azure AD

I Azure AD kan attributens tekniska namn avvika från namnen i det grafiska användargränssnittet. MPASSid hämtar uppgifterna via Microsoft Graph API. När uppgifterna hämtas på detta sätt, måste man känna till attributens tekniska namn och även gemener och versaler ska användas rätt i attributen (surname vs Surname).

Med hjälp av PowerShell-funktionen nedan kan du kontrollera attributens skrivsätt genom att till exempel hämta uppgifterna för någon av testkoderna i Azure AD. Vi rekommenderar att man först testar attributens skrivsätt på detta sätt.

Funktionen klipps och klistras i PowerShell-fönstret och hämtas därefter med kommandot `getAccountAttributes` i samma fönster.

```

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 )
}

```

```

# Exempel på användning av funktionen.
# Utan parametern -optionalAttributes hämtar kommandot basuppgifterna för användarobjektet (visningsnamn,
förnamn, efternamn och UPN).
# Du kan lägga till fler attributnamn i parametern -optionalAttributes; dessa ska separeras med kommatecken.
# Ange uppgifterna för App registration och Azure AD tenant som du skapade ovan som värden x, y, och z.

```

```

getAccountAttributes -clientID "xxxxxxxxxxxxxxxxxxxxxx" -clientSecret "yyyyyyyyyyyyyyyyyy" -tenantID
"zzzzzzzzzzzzzzzzzzzz" -userPrincipalName "<haettavatunnus@domain.onmicrosoft.com>" -optionalAttributes "city,
companyName,Department,department,faxNumber,jobTitle,officeLocation,onpremisesextensionattributes,postalCode,
state,streetAddress"

```