Hub.eduid.hu

Az o365.eduid.hu címen működő szolgáltatás utódja.

Célja: eduID-val rendelkező végfelhasználók számára biztosít automatikus felhasználó létrehozást és licensz kiosztást felhős szolgáltatásokban (jelenleg Microsoft licenszek kiosztása)

Microsoft integráció

Microsoft Graph API-n keresztül létrehozza a felhasználót és affiliation (student, staff, member) alapján hozzárendeli csoportokhoz. A csoporthoz hozzá lehet rendelni licenszeket, illetve jogosultságokat, amit automatikusan megörököl a felhasználó

Az o365.eduid.hu címen működő szolgáltatás utódja.

Célja: eduID-val rendelkező végfelhasználók számára biztosít automatikus felhasználó létrehozást és licensz kiosztást felhős szolgáltatásokban (jelenleg Microsoft licenszek kiosztása)

Szükséges beállítások Microsoft oldalról

1. Készítsünk egy Office 365 tenant-ot, ha még nincs: https://learn.microsoft.com/hu-hu/microsoft-365/education/deploy/create-your-office-365-tenant
2. A https://portal.azure.com oldalon bejelentkezve, hozzunk létre 1-1 biztonsági csoportot a tanulók és a dolgozók részére. Jegyezzük fel a csoportok objektumazonosítóját
3. Ahhoz, hogy a hub.eduid.hu szolgáltatás kezelni tudja a létrehozott tenant-ot, regisztráljunk egy új alkalmazást:
   https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/CreateApplicationBlade (ajánlott név: hub.eduid.hu) Mentsük el a generált "Alkalmazás (ügyfél) azonosítója" értéket
4. Az alkalmazáshoz készítsünk egy új titkos ügyfélkódot, majd a generálás végén mentsünk el a titkos ügyfélkód "Érték" mező értékét. bélyegkép
5. A létrehozott alkalmazáshoz állítsuk be a szükséges jogosultságokat:
   bélyegkép

- User.ReadWrite.All
- Group.ReadWrite.All
- Directory.ReadWrite.All
- GroupMember.ReadWrite.All
- MailboxSettings.Read
- MailboxSettings.ReadWrite

"Rendszergazda jogosultság megadása..." gombbal fogadjuk el az új beállításokat

6. A SAML login bekapcsolásának egyelőre sajnos nincs webes beállítási lehetősége, a Microsoft-tól sem kaptunk ezügyben iránymutatást, ezért ezt PowerShell-en keresztül kell megtenni.

Figyelem! Ha bekapcsoljuk a domain-ra a SAML alapú (Federated) bejelentkezést, akkor már csak azon keresztül lehet bejelentkezni az adott domainre, nincs lehetőség, vegyeshasználatra! Csak akkor hatjsuk végre a beállítást, ha rendben megtörtént a hub.eduid.hu és Microsoft közötti kapcsolat és megfelelően létrejöttek a felhasználók!

Indítsunk egy PowerShell-t, majd adjuk ki a *Connect-MsolService* parancsot (ha nincs még feltelepítve, akkor a Install-Module MSOnline paranccsal lehet). Jelentkezzünk be adminisztrátori fiókunkkal.



Állítsuk be az alábbi változókat:

```
$dom = _domain amire engedélyezzük a Federációs bejelentkezést_
$BrandName = _intézmény neve_
$LogOffUrl = _IdP kijelentkezési URL-je_
$ecpUrl = _IdP bejelentkezési URL-je_
$MyURI = _IdP entity ID-ja_
$MySigningCert = _IdP selfsigned tanúsítványa_
$Protocol = "SAMLP"
```

Példa:

```
$dom = "kifu.gov.hu"
$BrandName = "Kormányzati Informatikai Fejlesztési Ügynökség"
$LogOffUrl = "<https://idp.niif.hu/simplesaml/saml2/idp/SingleLogoutService.php>"
$ecpUrl = "<https://idp.niif.hu/simplesaml/saml2/idp/SSOService.php>"
$MyURI = "<https://idp.niif.hu/shibboleth>"
$MySigningCert = "MIID3zCCAsegAwIBAgI......XEhu3Otgo="
$Protocol = "SAMLP"
```

Majd futtassuk le:

```
Set-MsolDomainAuthentication -DomainName $dom -FederationBrandName $BrandName -Authentication Federated -PassiveLogOnUri $ecpUrl -ActiveLogOnUri $ecpUrl -SigningCertificate $MySigningCert -IssuerUri $MyURI -LogOffUri $LogOffUrl -PreferredAuthenticationProtocol $Protocol
```

Ha nem ad vissza semmilyen hibaüzenetet, akkor az office.com -ra való bejelentkezéssel tudjuk tesztelni. Miután beírtuk az e-mail címet a bejelentkező ablakban, akkor át fog irányítani a böngésző az IdP-nkre.

Bejelentkezési mód visszaállítása:

```
Set-MsolDomainAuthentication -DomainName $dom -Authentication Managed
```

Szükséges beállítások IdP oldalon

A korábbiakhoz képest nincs változás. Leírása: O365_SAML

Regisztrációja hub.eduid.hu szolgáltatásba

Az alábbi paramétereket kell megküldeni az ügyfélszolgálati e-mail címünkre (info@eduid.hu):

- teantID ("Bérlő azonosítója")
- domain nevek, ami alatt a felhasználókat létre kell hozni ("Egyéni tartománynevek"-nél felvett domain-ek, amiket kezelni kell)
- affiliation alapján melyik csoportokba helyezzük át a felhasználókat. Ehhez szükséges egy affiliation és groupID összerendelés (pl student-ek kerüljenek az XY csoportba)

- a létrehozott alkalmazáshoz tartozó "Alkalmazás (ügyfél) azonosítója" és a titkos ügyfélkód
- domain nevek, ami alatt a felhasználókat létre kell hozni

Jelszavakat, bizalmas információkat érdemes egyszer használatos linken keresztül küldeni, pl a https://pwpush.einfra.hu/ szolgáltatáson

---

Változat #1
document-uploader hozta létre 2025-08-07 12:10:55 CEST
document-uploader frissítette 2025-08-07 12:10:55 CEST