

# AAI\_AzureADasAuthsource

Amennyiben Azure AD-ban tároljuk a felhasználói adatokat, úgy lehetőség van azt azonosítási forrásként is használni. A [SimpleSAMLphp](#) oldalon leírt telepítés után az alábbiak elvégzésére van szükség:

(ez csak egy példakonfiguráció, természetesen el lehet ettől térni)

## Teendők SimpleSAMLPHP (SSP) oldalon

Keressük ki az Azure AD-ból a Tenant ID-t. A beállítás során erre *TenantID*-val fogunk hivatkozni, oda minden esetben ezt az azonosítót kell behelyettesíteni. Az azonosítót jelenleg a [https://portal.azure.com/#blade/Microsoft\\_AAD\\_IAM/ActiveDirectoryMenuBlade/Overview](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview) oldalon keresztül lehet beszerezni (Forrás: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-to-find-tenant>)

A *DOMAIN* helyére a használni kívánt scope-ot szükséges behelyettesíteni (pl *intezmeny.hu*)

## config/authsources.php fájlba

```
'default-sp' => [  
    'saml:SP',  
  
    // The entity ID of this SP.  
    // Can be NULL/unset, in which case an entity ID is generated based on the metadata URL.  
    'entityID' => null,  
  
    // The entity ID of the IdP this SP should contact.  
    // Can be NULL/unset, in which case the user will be shown a list of available IdPs.  
    'idp' => 'https://sts.windows.net/_TenantID_',  
  
    // The URL to the discovery service.
```

```

// Can be NULL/unset, in which case a builtin discovery service will be used.
'discoURL' => null,
'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent',
'simplesaml.nameidattribute' => 'eduPersonTargetedID',

/*
 * The attributes parameter must contain an array of desired attributes by the SP.
 * The attributes can be expressed as an array of names or as an associative array
 * in the form of 'friendlyName' => 'name'. This feature requires 'name' to be set.
 * The metadata will then be created as follows:
 * <md:RequestedAttribute FriendlyName="friendlyName" Name="name" />
 */
/*
'name' => [
    'en' => 'A service',
    'no' => 'En tjeneste',
],

'attributes' => [
    'attrname' => 'urn:oid:x.x.x.x',
],
'attributes.required' => [
    'urn:oid:x.x.x.x',
],
*/
],

```

## config/config-metarefresh.php fájlba

```

$config = [

'sets' => [
    'azure' => [
        'cron' => ['hourly'],
        'sources' => [
            [
                'src' => 'https://login.microsoftonline.com/_TenantID_/federationmetadata/2007-06/federationmetadata.xml',
            ]
        ]
    ]
]

```

```

    ],
  ],
  'expireAfter' => 34560060, // Maximum 4 days cache time (3600*24*4)
  'outputDir' => 'metadata/metarefresh-azure',
  'outputFormat' => 'flatfile',
],
],
];

```

## metadata/saml20-idp-hosted.php

A

```

'authproc' => [

  10 => [
    'class' => 'core:AttributeMap',
    'azure2name'
  ],

  15 => [
    'class' => 'core:AttributeCopy',
    'eduPersonPrincipalName' => 'schacPersonalUniqueCode',
  ],

  16 => ['class' => 'core:PHP',      'code' => '
$attributes[=
"urn:schac:personalUniqueCode:int:esi:_DOMAIN_:" .
$attributes["schacPersonalUniqueCode"]("schacPersonalUniqueCode")[0])[0];
',
  ],

  18 => [
    'class' => 'core:AttributeAlter',
    'subject' => 'eduPersonPrincipalName',
    'pattern' => '/^.*$/ ',
    'replacement' => '${0}@_DOMAIN_',
    'target' => 'eduPersonPrincipalName'
  ],

```

```
20 => [  
  'class' => 'core:AttributeAdd',  
  'eduPersonEntitlement' => array('urn:mace:dir:entitlement:common-lib-terms')  
],
```

```
22 => [  
  'class' => 'core:AttributeAdd',  
  'schacHomeOrganization' => array('_DOMAIN_')  
],
```

```
23 => [  
  'class' => 'core:AttributeAdd',  
  'schacHomeOrganizationType' =>  
array('urn:schac:homeOrganizationType:eu:higherEducationalInstitution')  
],
```

// Azure AD-ban célszerű az affiliation-t (intézményhez való viszonyt, pl hallgató, oktató, dolgozó) security group alapján meghatározni. Ezeknek az objektum azonosítóját át fogja adni az Azure AD, amit könnyen kicserélhetünk a kívánt affiliation-re:

```
31 => [  
  'class' => 'core:AttributeAlter',  
  'subject' => 'eduPersonAffiliation',  
  'pattern' => '/^_eduID_Dolgozó_GroupID_$/', // _eduID_Dolgozó_GroupID_ értéket cseréljük a megfelelő  
Objektum ID-ra  
  'replacement' => 'faculty',  
],
```

```
32 => [  
  'class' => 'core:AttributeAlter',  
  'subject' => 'eduPersonAffiliation',  
  'pattern' => '/^_eduID_Hallgató_GroupID_$/', // _eduID_Hallgató_GroupID_ értéket cseréljük a megfelelő  
Objektum ID-ra  
  'replacement' => 'student',  
],
```

```
33 => [  
  'class' => 'core:AttributeAlter',  
  'subject' => 'eduPersonAffiliation',
```

```
'pattern' => '/^_eduID_Admin_GroupID_$/', // _eduID_Admin_GroupID_ értéket cseréljük a megfelelő
```

Objektum ID-ra

```
'replacement' => 'staff',
```

```
],
```

```
34 => [
```

```
  'class' => 'core:AttributeAdd',
```

```
  'eduPersonAffiliation' => array('member'),
```

```
],
```

```
35 => [
```

```
  'class' => 'core:AttributeCopy',
```

```
  'eduPersonAffiliation' => 'eduPersonScopedAffiliation'
```

```
],
```

```
36 => [
```

```
  'class' => 'core:AttributeAlter',
```

```
  'subject' => 'eduPersonScopedAffiliation',
```

```
  'pattern' => '/^.*$/',
```

```
  'replacement' => '${0}@$_DOMAIN_',
```

```
],
```

```
50 => [
```

```
  'class' => 'core:TargetedID',
```

```
  'identifyingAttribute' => 'eduPersonPrincipalName',
```

```
  'nameId' => TRUE,
```

```
],
```

```
60 => [
```

```
  'class' => 'core:AttributeMap',
```

```
  'name2oid'
```

```
],
```

```
75 => [
```

```
  'class' => 'entitycategories:EntityCategory',
```

```
  'default' => true,
```

```
  'strict' => false,
```

```
  'allowRequestedAttributes' => true,
```

```
  'http://eduid.hu/category/registered-by-eduidhu' => [],
```

```
  'http://www.geant.net/uri/dataprotection-code-of-conduct/v1' => [
```

```

        'urn:oid:2.16.840.1.113730.3.1.241', # displayName
        'urn:oid:2.5.4.4', # sn
        'urn:oid:2.5.4.42', # givenName
        'urn:oid:0.9.2342.19200300.100.1.3', # mail
        'urn:oid:1.3.6.1.4.1.5923.1.1.1.6', # eduPersonPrincipalName
        'urn:oid:1.3.6.1.4.1.5923.1.1.1.9', # eduPersonScopedAffiliation
        'urn:oid:1.3.6.1.4.1.5923.1.1.1.1', # eduPersonAffiliation
    ],
    'http://refeds.org/category/research-and-scholarship' => [
        'urn:oid:2.16.840.1.113730.3.1.241', # displayName
        'urn:oid:2.5.4.4', # sn
        'urn:oid:2.5.4.42', # givenName
        'urn:oid:0.9.2342.19200300.100.1.3', # mail
        'urn:oid:1.3.6.1.4.1.5923.1.1.1.6', # eduPersonPrincipalName
        'urn:oid:1.3.6.1.4.1.5923.1.1.1.9', # eduPersonScopedAffiliation
        'urn:oid:1.3.6.1.4.1.5923.1.1.1.1', # eduPersonAffiliation
    ],
],

90 => 'core:AttributeLimit',

'simplesaml.nameidattribute' => 'urn:oid:1.3.6.1.4.1.5923.1.1.1.6',

'attributeencodings' => array(
    'urn:oid:1.3.6.1.4.1.5923.1.1.1.10' => 'raw', /* eduPersonTargetedID with oid NameFormat. */
),

'sign.logout' => true
];

```

## attributemap/azure2oid.php

```

<?php
$attributemap = [
    // displayName
    'http://schemas.microsoft.com/identity/claims/displayname' => 'urn:oid:2.16.840.1.113730.3.1.241',

```

```

// eppn
'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name' => 'urn:oid:1.3.6.1.4.1.5923.1.1.1.6',
// givenName
'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname' => 'urn:oid:2.5.4.42',
// cn
'://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname' => 'urn:oid:2.5.4.3',
// surname
'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname' => 'urn:oid:2.5.4.4',
// mail
'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress' =>
'urn:oid:0.9.2342.19200300.100.1.3',
// o & organisation
'http://schemas.microsoft.com/identity/claims/tenantid' => 'urn:oid:2.5.4.10',
];

```

## attributemap/azure2name.php

```

<?php
$attributemap = [
    // eppn
    'http://schemas.microsoft.com/identity/claims/objectidentifier' => 'eduPersonPrincipalName',
    // mail
    'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress' => 'mail',
    // displayName
    'http://schemas.microsoft.com/identity/claims/displayname' => 'displayName',
    // givenName
    'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname' => 'givenName',
    // cn
    'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname' => 'sn',
    // affiliation
    'http://schemas.microsoft.com/ws/2008/06/identity/claims/groups' => 'eduPersonAffiliation',
];

```

## Teendők Azure AD oldalon

1. A <https://portal.azure.com/> oldalon jelentkezünk be egy adminisztrátori fiókkal
2. Válasszuk az "App registrations"-t

- 3. "New registration"
- 4. "Redirect URI (optional)" -nál adjuk meg a telepített SSP default SP címét. Pl: <https://idp.DOMAIN/simplesaml/module.php/saml/sp/metadata.php/default-sp>
- 5. "Token configuration" # > "Add optional claim"> "Token type"-nál válasszuk a "SAML"-t és jelöljük ki az összes attribútumot, majd, "Add"
- 6. "Add groups claim", majd mentsük el

Search (Ctrl+/)

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

+ Add optional claim

+ Add groups claim

Claim	Description	Token type	Optional settings
acct	User's account status in tenant	SAML	-
email	The addressable email for this user, if the user has one	SAML	-
groups	Optional formatting for group claims	ID, Access, SAML	Default
upn	An identifier for the user that can be used with the username_hint parameter; not a durable identifier for ...	SAML	Default

7. Állítsuk be az API permissions-t az alábbi alapján:

Search (Ctrl+/)

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions shows all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

Grant admin consent for Színház- és Filmművészeti Egyetem

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (5)				
email	Delegated	View users' email address	No	Granted for
GroupMember.Read.All	Delegated	Read group memberships	Yes	Granted for
openid	Delegated	Sign users in	No	Granted for
profile	Delegated	View users' basic profile	No	Granted for
User.Read	Delegated	Sign in and read user profile	No	Granted for

To view and manage permissions and user consent, try [Enterprise applications](#).

Teszt

Változat #3  
cziernorbert hozta létre 9 április 2025 16:37:14  
cziernorbert frissítette 10 április 2025 09:55:10