EntraID in eduID.hu

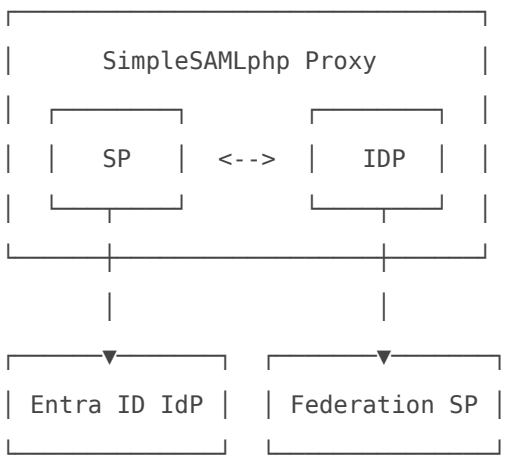
Overview

This document explains how to configure SimpleSAMLphp so that it uses Microsoft Entra ID as the authentication authority (Identity Provider) and then acts as a SAML Identity Provider (IdP) to external federated Service Providers (SPs). This pattern is commonly known as an **authentication proxy** or **IdP proxy**.

In plain terms:

- End users authenticate against **Entra ID**.
- SimpleSAMLphp receives this authentication and optionally enriches or transforms attributes.
- SimpleSAMLphp then issues SAML assertions to federation partners or internal applications.

The proxy setup looks like this:



Configure a SimpleSAMLphp SAML 2.0 Service Provider

To configure SimpleSAMLphp as a SAML 2.0 Service Provider, a new authentication source must be defined in the file `config/authsources.php`. This authentication source represents SimpleSAMLphp in its SP role towards Entra ID and is used to publish SP metadata.

The following example shows a minimal configuration suitable for use with Microsoft Entra ID:

```
$config = [
    /* ... */
    /* An authentication source that can authenticate against SAML 2.0 IdPs. */
    'entraid-sp' => [
        'saml:SP',
        // The entity ID of this SP.
        'entityID' => 'https://proxy.example.org/simplesaml',
        // The entity ID of the IdP this SP should contact.
        'idp' => 'https://sts.windows.net/<your-entra-tenant-id>/'
        'name' => ['en' => 'Microsoft Entra ID'],
        // certificates
        'certificate' => 'server.crt',
        'privatekey' => 'server.key',
        'privatekey_pass' => 'YourPrivateKeyPassphrase', /* you encrypt your private key,
right? */
        'authproc' => [
            /* authproc rules*/
        ],
        // fine tuning the auth source for Entra ID
        'sign.authnrequest' => true,
        'sign.logout' => true,
        'proxymode.passAuthnContextClassRef' => true,
        'disable_scoping' => true,
        'signature.algorithm' => 'http://www.w3.org/2001/04/xmldsig-more#rsa-sha256',
    ],
],
```

Configure SimpleSAMLphp SAML 2.0 Identity Provider

In order for SimpleSAMLphp to issue SAML assertions to downstream Service Providers, it must be configured as a SAML 2.0 Identity Provider. This configuration is defined in the file `metadata/saml20-idp-hosted.php`.

The IdP configuration references the previously defined authentication source, effectively chaining authentication to Entra ID.

```
$metadata['http://proxy.example.org/idp'] = [
   /*
    * The hostname of the server (VHOST) that will use this SAML entity.
    *
    * Can be '__DEFAULT__', to use this entry by default.
    */
   'host' => '__DEFAULT__',
   // X.509 key and certificate. Relative to the cert directory.
   'privatekey' => 'server.pem',
   'privatekey_pass' => 'YourPrivateKeyPassphrase',
   'certificate' => 'server.crt',
   /*
    * Authentication source to use. Must be one that is configured in
    * 'config/authsources.php'.
    */
   'auth' => 'entraid-sp', // proxy to Microsoft Entra ID
   'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-format:uri',
   'authproc' => [
   ],
];
```

Create a new Enterprise Application in Entra ID

1. Create a new Enterprise Application

A new **Enterprise Application** must be created in the Entra ID portal to represent SimpleSAMLphp in its role as a SAML Service Provider. This can be done by navigating to the **Enterprise applications** section of the Entra ID portal and creating a new application. During creation, the option to create a custom application that is not found in the gallery should be selected. A descriptive name and also select *Integrate any other application you don't find in the gallery*.

2. Configure SAML-based Single Sign-On

After the application has been created, SAML-based single sign-on must be enabled. This is done by opening the application, navigating to the **Single sign-on** section, and selecting **SAML** as the sign-on method. The trust relationship between Entra ID and SimpleSAMLphp is established by

uploading the SAML 2.0 SP metadata generated by SimpleSAMLphp. The metadata upload automatically populates the basic SAML configuration, including the entity ID and assertion consumer service URL.

3. Download Entra ID Federation Metadata

To finalise the SimpleSAMLphp side of the bilateral trust relationship between your Entra ID tenant and SimpleSAMLphp, copy your Enterprise Application's *App Federation Metadata*. Using SimpleSAMLphp's Metadata Converter (found on the *Federation* tab of SimpleSAMLphp's admin portal), convert your App Federation Metadata to SimpleSAMLphp's native PHP format. Once you have the converted metadata, paste it into the `metadata/saml20-idp-remote.php` file.

4. Configure Attribute Claims Rules

Attribute and claim mappings can be adjusted in the Entra ID application to ensure that the required user attributes are released to SimpleSAMLphp. These attributes will later be available for transformation, filtering, or enrichment before being sent to downstream Service Providers.

Attribute Mapping and Transformation

When authenticating against Microsoft Entra ID, user attributes are returned as SAML claims using Microsoft-specific or WS-Federation-style claim URIs. In most federation environments, these claims must be mapped to standard SAML or eduPerson attribute names before they are released to downstream Service Providers.

SimpleSAMLphp performs attribute mapping through authentication processing filters. Mapping rules are applied in the `authproc` section of the authentication source that represents Entra ID, ensuring that attributes are normalized as soon as they enter SimpleSAMLphp. These mappings can either reuse
[https://github.com/simplesamlphp/simplesamlphp/blob/master/attributemap/entra2name.php built-in attribute maps provided] by SimpleSAMLphp or be defined explicitly using custom rules.

Here is an example of using `core:AttributeMap` processing filter:

```
'authproc' => [
    /* ... */
    60 => [
        'class' => 'core:AttributeMap',
        /* there are several versions of the userprincipalname claim, you only need the one
you use */
        'http://schemas.xmlsoap.org/claims/UPN' => 'eduPersonPrincipalName',
```

```
        'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn' =>
'eduPersonPrincipalName',
        'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name' =>
'eduPersonPrincipalName',
        /* other possible attributes */
        'http://schemas.xmlsoap.org/claims/CommonName' => 'displayName',
        'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname' => 'givenName',
        'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname' => 'sn',
        'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress' => 'mail',
        'http://schemas.microsoft.com/ws/2008/06/identity/claims/groups' => 'memberOf',
    ],
    /* ... */
],
```

or

```
'authproc' => [
    60 => [
'class' => 'core:AttributeMap',
'attributemap' => 'entra2name',
    ],
],
```

Once mapped, attributes can be further filtered, enriched, or selectively released by additional authentication processing filters before being issued by the proxy IdP.

Configure SimpleSAMLphp to Use Entra ID as an Authentication Source

With the Enterprise Application configured, SimpleSAMLphp must be instructed to use Entra ID as its authentication source. This is done by setting the IdP entity ID in the entraid-sp authentication source to the Entra ID tenant identifier.

```
'idp' => 'https://sts.windows.net/<your-entra-tenant-id>/',
```

This configuration causes SimpleSAMLphp, acting as a Service Provider, to redirect authentication requests to Entra ID. After importing the Entra ID metadata, the corresponding entity ID should be visible under SAML 2.0 IdP metadata on the Federation tab of the SimpleSAMLphp admin interface.

Testing

You should now be able to go to the **Test** tab in the admin portal, log in to your `entraid-sp` authentication source, and be redirected to your Entra ID application’s login page. Once logged in, it is worth verifying that SimpleSAMLphp is correctly receiving the attributes from Entra ID.

Sources

- https://nathansenblog.wordpress.com/2021/02/23/azure-ad-single-sign-on-with-simplesamlphp
- https://safire.ac.za/technical/resources/configuring-simplesamlphp-to-use-entra-id

---

Változat #2
cziernorbert hozta létre 2026-04-13 09:32:58 CEST
cziernorbert frissítette 2026-04-13 09:39:29 CEST