Configuring Microsoft Azure as an authentication provider for OpenAthens

This section assumes a basic level of familiarity with the Azure interface. Whilst our service desk will always try to be helpful, they can only support the OpenAthens end of the connection.

Preparation

You will need

- Access to your Microsoft Azure portal
- Access to the OpenAthens admin interface as the domain administrator

Method:

Add an application to Azure

1. Go to **Active Directory > Enterprise applications > All applications** section, click the new application button, search for and select OpenAthens.
2. Download and save your Azure metadata from the signing certificate section via the 'Metadata XML' link

3. Still within the application you are creating, select the users and groups option > add to configure who will be able to access OpenAthens. You should enable at least your own test account at this stage. You can enable additional users or groups later.

Configure OpenAthens settings

For complete details see the SAML connector page, but the short version is:

1. Log into the OpenAthens admin area as the domain administrator

2. Go to Management > Connections > Add and select the SAML connector

3. Upload the metadata file you saved from Azure earlier

4. Save

5. In the display name mapping field enter: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`
   This represents a standard value in Azure known as UPN that is usually suitable. You can change this later at any time before you go live.

6. Set the unique user mapping to use Subject NameID instead of an attribute by using the radio button. The identifiers that OpenAthens passes to resources for your users is based on this, so if you want to select a different attribute as the unique identifier you will want to do so before you roll this out to your users.

7. Go to the </>relying party tab and copy the link displayed there - it will look similar to:

   ```
   https://login.openathens.net/saml/2/metadata-sp/yourdomain.com/la/1234
   ```

8. Finally: set the status and save.

    a. If you have no existing OpenAthens users you can select live, visible and default under status and start testing as soon as you have saved.

    b. If you have existing OpenAthens users, leave those three checkboxes cleared when you save or you will stop existing users from being able to sign in. You can still test, but will need to use debug mode - see: How to use debug mode.

Finish the basic set-up in Azure

1. On the OpenAthens application integration page select the single sign-on option and set:

    a. Single Sing-on Mode > select 'SAML-based Sign-on'.

    b. OpenAthens Domain and URL > Identifier > enter the link you copied from the relying party tab earlier and save

You should now be able to test that signing in works and will be ready to add any additional bits you need.

Set up any additional attributes you need to send to OpenAthens

You may want to be able to do more with OpenAthens than simply sign the user in - for example you can assign permissions based on the values of the attributes you send.

In Azure

1. In the OpenAthens application you set up in the Azure portal, go to the user attributes section and see if the attribute you want to send us is already available.
    a. If it is, copy the name for later then move on to the OpenAthens step. The attribute name is case sensitive and in Azure it will usually start with http://schemas.xmlsoap.org/ws/2005/05/identity/claims/...
    b. If the attribute is not already these, select the view and edit all other user attributes checkbox where you can add it - see: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-saml-claims-customization

In OpenAthens

1. See: Attribute mapping
2. See: Permission set rules

OpenAthens will cache these attributes when the user signs in, so changes in Azure won't be picked up until the next time the user starts an OpenAthens session.