Sign in to a generic application using OpenAthens

This will show you how in general to get a third party application that supports SAML to accept OpenAthens logins. You will only need to do this if the resource is not in a connected federation, or if it only supports one-to-one SAML connections.

Prerequisites

- Access to the configuration area of the application
- The application must make its SAML metadata available
- Access to the OpenAthens administration area at the domain level

Method

Application SSO settings

These are usually found under sections called things like Single-sign-on, SAML, Login options, Identity Provider, and similar. 'SAML' is usually the thing to look up in their documentation if that is available. If SAML is a separate component or plugin, you may need to add or update it.

The configuration will usually ask for some SAML metadata, but some may instead ask you to specify some Endpoint URLs and upload a certificate.

Metadata method

If they ask for this it will either be the URL of the metadata they need, or you may have to download it yourself to a file and then upload it to them.

The URL will be: `https://login.openathens.net/saml/2/metadata-idp/yourdomain.com`

... where `yourdomain.com` is your OpenAthens API name. It is usually the same as your scope which can be looked up on your organisation summary (i n the menu bar).

If you have downloaded it as a file, any text file extension is usually ok, but the application may insist on a .xml extension.

Endpoint method

They may want some or all of these:

Field might be called	Enter
SSO URL / address / endpoint Sign-in page URL/ address / endpoint	`https://login.openathens.net/saml/2/sso/yourdomain.com`
Sign-out page URL / address	`https://login.openathens.net/signout`
Change password URL / address	`https://login.openathens.net/auth#forgottenpassword`

... where `yourdomain.com` is your OpenAthens API name. It is usually the same as your scope which can be looked up on your organisation summary (i n the menu bar).

It will probably ask for a certificate and you will need to upload the x509 certificate that is published in your metadata (`https://login.openathens.net/saml/2/metadata-idp/yourdomain.com`) by copying it into a file then topping and tailing it as follows:

```
-----BEGIN CERTIFICATE-----
ThisIsAnExampleNotARealOneANBgkqhkiG9w0BAQsFADCBoDEoMCYGCSqGSIb3DQEJARYZYXRo
ZW5zaGVscEBlZHVzZXJ2Lm9yZy51azELMWkGA1UEBhMCR0IxETAPBgNVBAgMCFNvbWVyc2V0MQ0w
CwYDVQQHDARCYXRoMRAwDgYDVQQKDAdFAIVzZXJ2MRMwEQYDVQQLDApPcGVuQXRoZW5zMR4wHAYD
VQQDDBVnYXRld2F5LmF0aGVuc2Ftcy5uCNQwHhcNMTUwMjI0MDkyMDA2WhcNMjUwMjI0MDkyMDA2
WjCBoDEoMCYGCSqGSIb3DQEJARYZYXRoSD5zaGVscEBlZHVzZXJ2Lm9yZy51azELMAkGA1UEBhMC
R0IxETAPBgNVBAgMCFNvbWVyc2V0MQ0wROYDVQQHDARCYXRoMRAwDgYDVQQKDAdFZHVzZXJ2MRMw
EQYDVQQLDApPcGVuQXRoZW5zMR4wHAYDUWQDDBVnYXRld2F5LmF0aGVuc2Ftcy5uZXQwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBLSCandpa4o0Njtw1DqbrrNTfOVe1PqyXIIVmDrJ6VUR/
mokXXu+m5Gm+1f+Tfas4986s98hoff76ES46hd764asjgzrdsfl84S3en1pdXKsH1WnUnVWUmpl9
WJZrUwi5i8X80LNyr7PmudhuKNEATGUXkUuxWCkk2d8jf91hy7Qu+HA8LOKtdbbNigErh2IY/YuN
WUVUqgGbMH5BGr7ZEhPrz+Vwcf9lhPW+tCpKpZEzJfQiq8EoPaeMXEpKWBEErm67gkWFCA5VhfcJ
LqFjQEC3pWOxt5rZVS8gl/Z33VSJZVzY5KWcQzmGaLXPHXyiKPmixl6+DjGlUM0ylNF7GvtDAgMB
AAEwDQYJKoZIhvcNAQELBQADggEBAFhmhSjLZueiJ6F7mQCpfB0Hj4Y8FyFUUc8NMAt5Set7H4DK
SSl4shcqisZBa5yTdyenYwkmBszvCWs6Yeep+zJmCR62cb/f1M32oMzLm02OlznWMkE8/IajGmdx
TnB6Z/XcdMMIiCeok4kqe5KMd5oRAyNskHYZ+8kzhs2zTveR+rqCtYxa/AYpwf7n0VQR9clBSNCI
T4BCRi10aPE531VIxl4ljY3CwNoZ4lQTU/0aj8O4j68V2neiQb8lewAii0b2xoyOGYP4okd7T2tl
4gl2noVbCvYNjd6GYze/w4lgwiemkby7wu5sN1lEudgKDV+H54wU29ZIyDEFM6DDNE4=
-----END CERTIFICATE-----
```

For more information about your metadata, see how to access your login.openathens.net metadata.

Identifiers

Make a note of any identifiers the system needs you to pass to it and the specific, case sensitive name it wants you to send it as. OpenAthens can send attributes under any name. (See Attribute release)

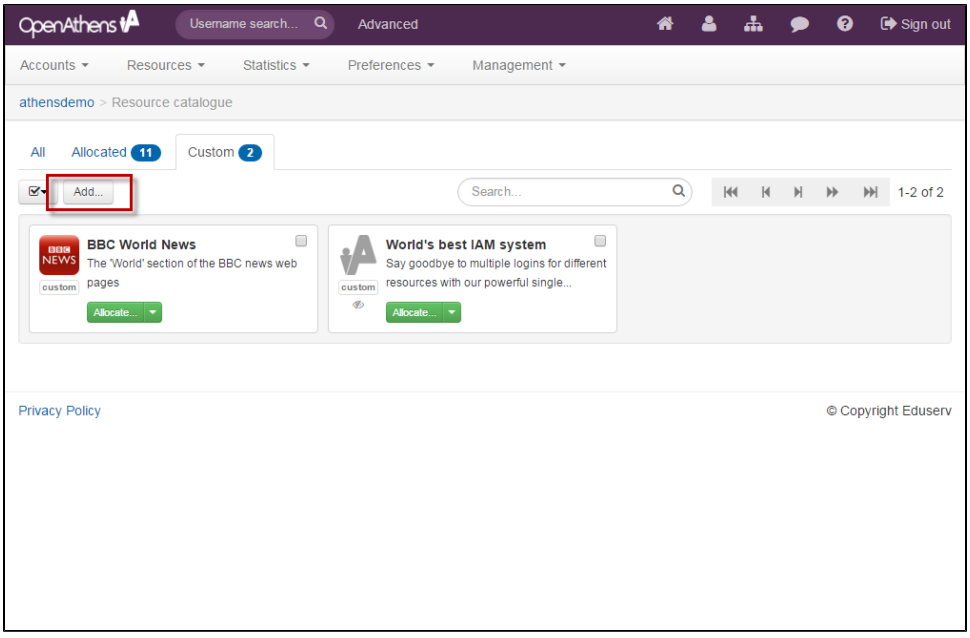
Some systems will let you specify the attribute name - if so then then using OpenAthens attribute names will likely be easiest. The common ones are:

- username
- emailAddress
- forenames
- surname

You will also need the application's SAML metadata, either as a web address or a downloaded file when you set up the custom SAML resource in OpenAthens.

Set up the custom SAML resource in OpenAthens

1. Access the administration area as the domain administrator and navigate to the catalogue (***Resources > Catalogue***).
2. Switch to the custom tab and click on the Add button



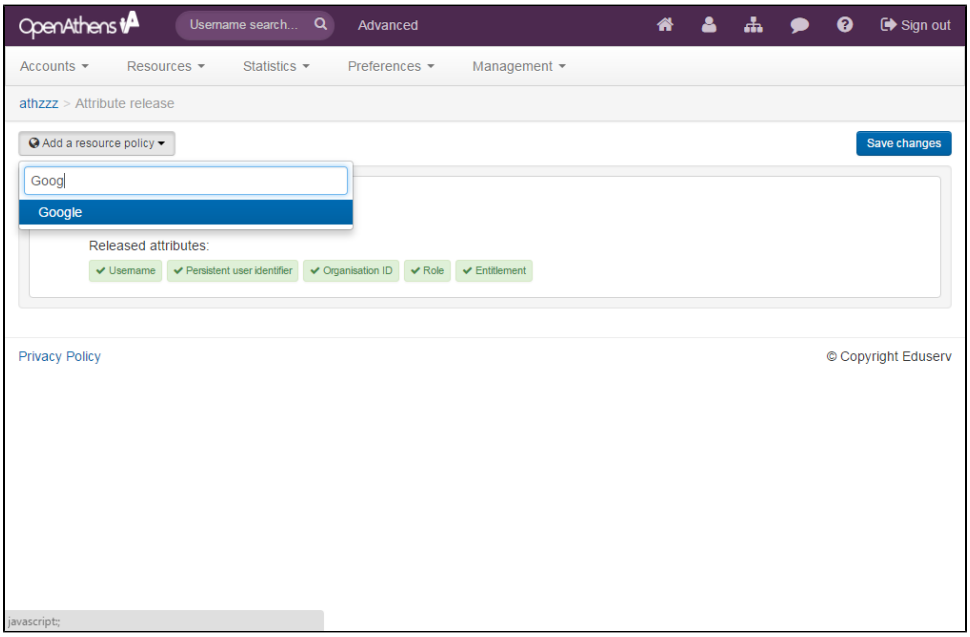
3. Select the SAML option

4. Enter the metadata address of the application or upload the metadata file
5. Click the create button

This will create the basic custom resource using the values in the metadata. If it doesn't have a suitable name, you can edit the details to change it, and add a description or logo.

Add the application to your release policy

1. Still in the administration area navigate to the release policy page (***Preferences > Attribute release***) and see if the attributes released under the Global policy are sufficient (these are the attributes that you send to all resources). If they are - e.g. the application needs standard federation identifiers such as targetedID and role - then you you can skip this section and start testing.



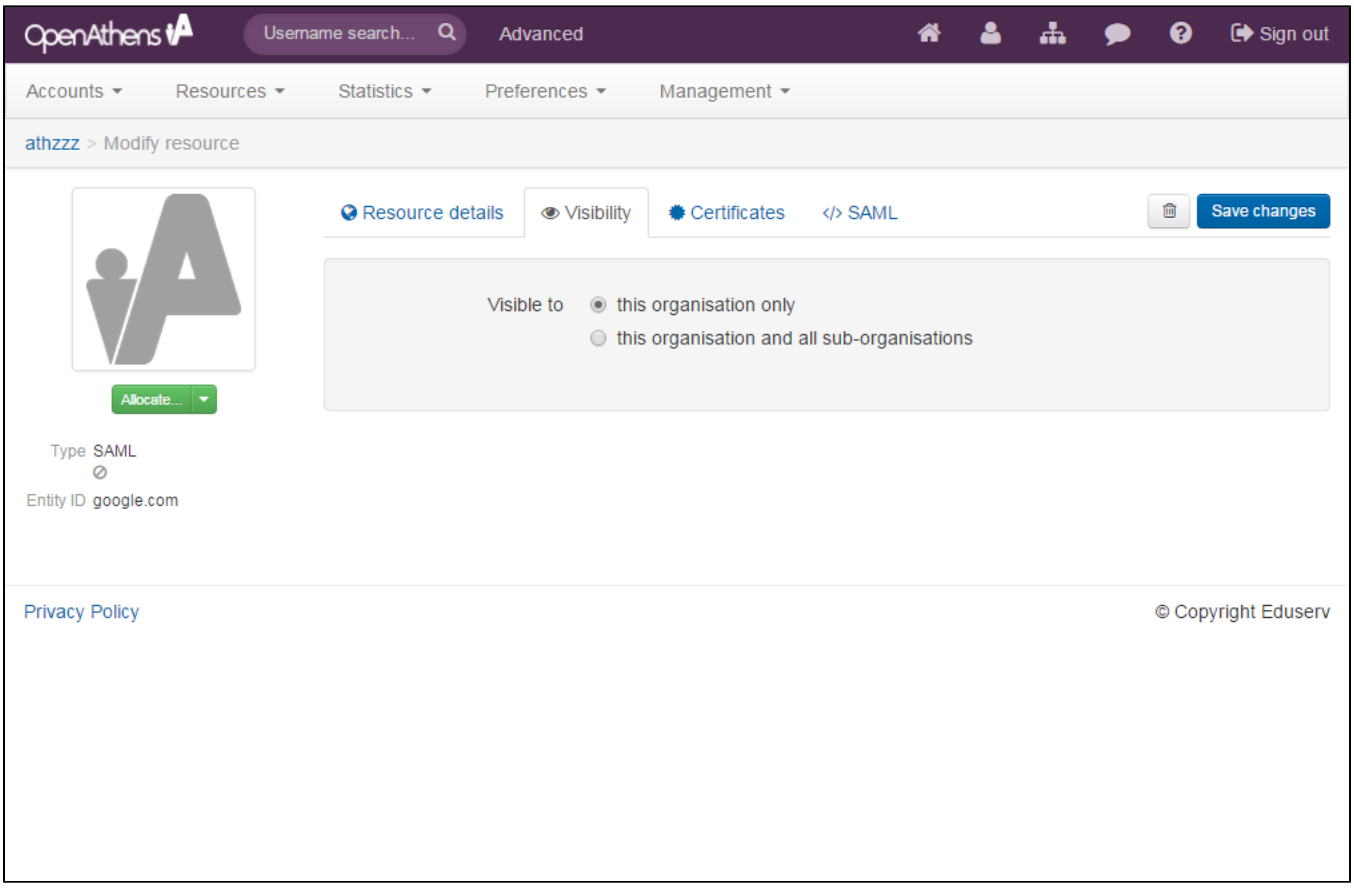
2. Add a resource policy via the button
    a. Start typing the name of the SAML resource.
    b. Select it from the list of any options to add a policy
3. Click on the attributes you want to release. You can change the names if you need to using the advanced button at the bottom of the policy, but you still need to click them here.
4. If your application's documentation mentions the SAML NameID at all, you may need to change the format we send it as. This is also done under the advanced button. E.g. if your application was using email address as the main identifier, you might need to change the Name ID to be:
    a. NameID format - `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
    b. NameID attribute: `Email address`
5. Click done and then save changes

This will now release the attribute that your application is expecting. This will only release them to the specified application.

Customise

Once the basic resource exists, that is all the system need to work unless you are using restrictive mode (see below). You can edit the details of the custom SAML resource in any way you need to.

All types of custom resources can be made available to sub-organisations by opening the detail view and changing the setting on the visibility tab:



Restrictive mode

If you are running in restrictive mode, the SAML resource MUST be included in at least one of the permission sets used by anyone who should gain access. If not then OpenAthens will block access at the authentication point.

If you have sub-organisations you MUST ALSO set the visibility setting described above and allocate it to permission sets under those sub-organisations. The cascade option may be useful.

Whilst our service desk will always try to be helpful, they can only support the OpenAthens end of this kind of connection.