Sign in to G Suite with OpenAthens

This is an example using G Suite (formally Google Apps) of how to set up a custom SAML resource so that you can log in using the hosted version of OpenAthens.

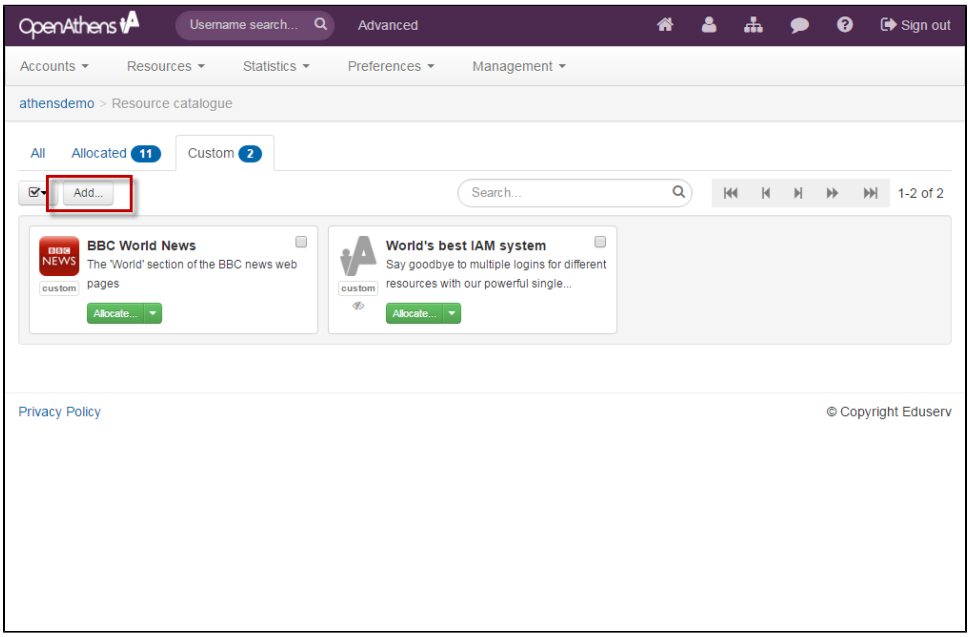
Prerequisites

- A G Suite domain
- Access to the G Suite admin dashboard
- Access to the OpenAthens administration area at the domain level

Method

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 google apps metadata address

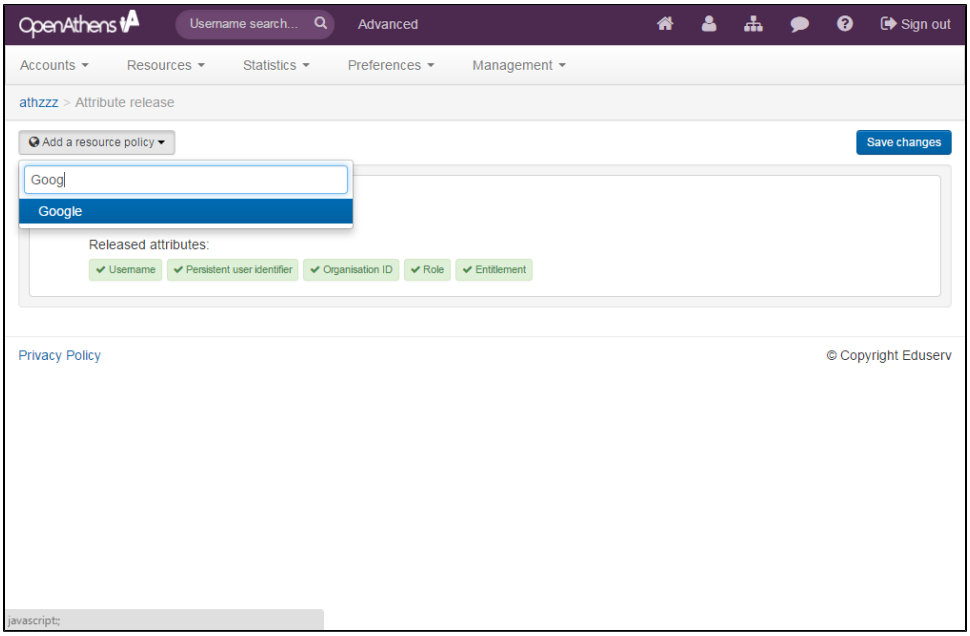
```
https://help.openathens.net/metadata/google.com/a/<GOOGLEAPPSDOMAIN>
```

5. Click the create button

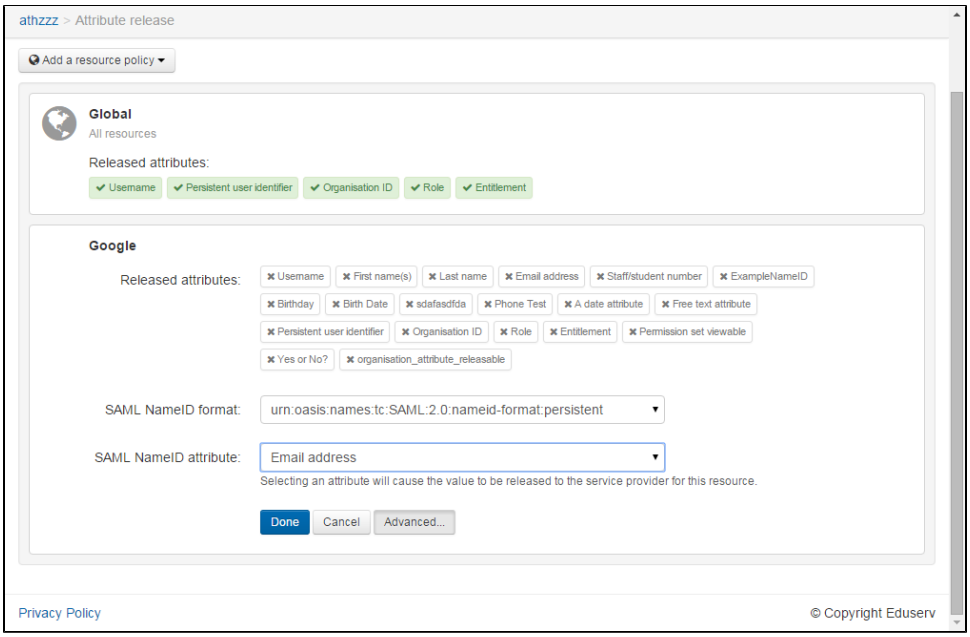
This will create the basic custom resource. We can come back and add details later if we need to.

Add G Suite to your release policy

1. Still in the administration area navigate to the release policy page (***Preferences > Attribute release***)



2. Add a resource policy via the button
    a. Start typing the name you gave the SAML resource. This will be 'Google' unless you have changed it.
    b. Select it from the list of any options to add a policy
3. Click the advanced button to access the NameID settings:



4. Set the SAML NameID format and attributes from the drop down boxes as:
    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 email attribute that Google are expecting as the username. This will only release it to Google. The email address on the OpenAthens account will need to match up with the email addresses stored at the Google end.

Access G Suite SSO settings

Access the SSO settings on the Google Apps dashboard. At the time of writing this was under the security section.

The section you are looking for is to do with setting up SSO with a third party identity provider - you will need to fill in the following fields:

Field	Enter
Sign-in page URL	https://login.openathens.net/saml/2/sso/<OPENATHENSDOMAIN> e.g. https://login.openathens.net/saml/2/sso/institution.ac.uk
Sign-out page URL	https://login.openathens.net/signout
Change password URL	https://login.openathens.net/auth#forgottenpassword

<OPENATHENSDOMAIN> can be looked up on your organisation summary (in the menu bar). It is usually the same as the internet domain used as your scope

You will need to upload the x509 certificate that is published in your metadata by copying it into a file then topping and tailing it as follows:

```
-----BEGIN CERTIFICATE-----
ThisIsAnExampleNotARealOneANBgkqhkiG9w0BAQsFADCBoDEoMCYGCSqGSIb3DQEJARYZYXRo
ZW5zaGVscEBlZHVzZXJ2Lm9yZy51azELMAkGA1UEBhMCR0IxETAPBgNVBAgMCFNvbWVyc2V0MQ0w
CwYDVQQHDARCYXRoMRAwDgYDVQQKDAdFZHVzZXJ2MRMwEQYDVQQLDApPcGVuQXRoZW5zMR4wHAYD
VQQDDBVnYXRld2F5LmF0aGVuc2Ftcy5uZXQwHhcNMTUwMjI0MDkyMDA2WhcNMjUwMjI0MDkyMDA2
WjCBoDEoMCYGCSqGSIb3DQEJARYZYXRoZW5zaGVscEBlZHVzZXJ2Lm9yZy51azELMAkGA1UEBhMC
R0IxETAPBgNVBAgMCFNvbWVyc2V0MQ0wCwYDVQQHDARCYXRoMRAwDgYDVQQKDAdFZHVzZXJ2MRMw
EQYDVQQLDApPcGVuQXRoZW5zMR4wHAYDVQQDDBVnYXRld2F5LmF0aGVuc2Ftcy5uZXQwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCandpa4o0Njtw1DqbrrNTfOVe1PqyXIIVmDrJ6VUR/
mokXXu+m5Gm+1f+Tfas4986s98hoff76s946hd764asjgzrdsfl84S3en1pdXKsH1WnUnVWUmpl9
WJZrUwi5i8X80LNyr7PmudhuKNEATGUXkAuxWCkk2d8jf91hy7Qu+HA8LOKtdbbNigErh2IY/YuN
WUVUqgGbMH5BGr7ZEhPrz+Vwcf9lhPW+tKpKpZEzJfQiq8EoPaeMXEpKWBEErm67gkWFCA5VhfcJ
LqFjQEC3pWOxt5rZVS8gl/Z33VSJZVzY5jWcQzmGaLXPHXyiKPmixl6+DjGlUM0ylNF7GvtDAgMB
AAEwDQYJKoZIhvcNAQELBQADggEBAFhmhujLZueiJ6F7mQCpfB0Hj4Y8FyFUUc8NMAt5Set7H4DK
SSl4shcqisZBa5yTdyenYwkmBszvCWs6Yeep+zJmCR62cb/f1M32oMzLm02OlznWMkE8/IajGmdx
TnB6Z/XcdMMIiCeok4kqe5KMd5oRAyNskHYZ+8kzhs2zTveR+rqCtYxa/AYpwf7n0VQR9clBSNCI
T4BCRi10aPE531VIxl4ljY3CwNoZ4lQTU/0aj8O4j68V2neiQb8lewAii0b2xoyOGYP4okd7T2tl
4gl2noVbCvYNjd6GYze/w4lgwiemkby7wu5sN1lEudgKDV+H54wU29ZIyDEFM6DDNE4=
-----END CERTIFICATE-----
```

You can access your SAML2 metadata for this at https://login.openathens.net/saml/2/metadata-idp/<OPENATHENSDOMAIN>. For details, see how to access your login.openathens.net metadata.

Save the details and you are ready to test.

Test

Once both ends are set up, you can try access at https://mail.google.com/a/<GSUITEDOMAIN> (www.google.etc will always use the google account rather than redirecting so you need to use one of the apps' subdomains). Unless you already have an active google session you should be directed to your organisation's OpenAthens sign in location - see about the authentication point.

The email address stored on OpenAthens accounts you sign in with must match up with the email addresses in Google Apps or no access is given.

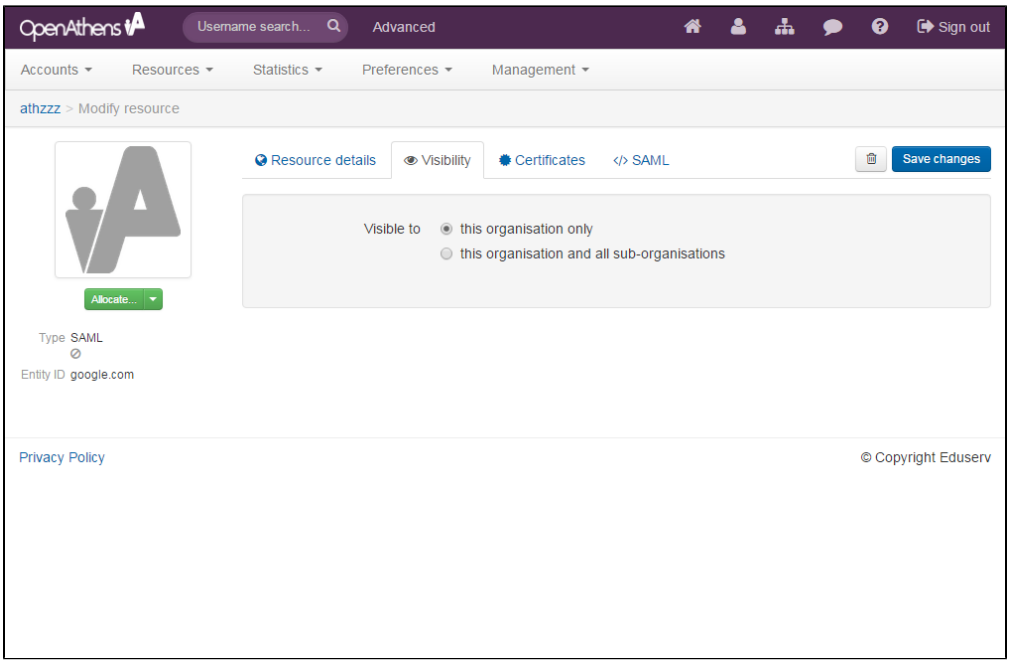
Toggle use on and off via Google's settings until you are ready to go live.

Customise

Once the basic resource exists, that is all the system needs to work unless you are using restrictive mode (see below).

If you want specific app target resources to appear in MyAthens for your users you can add regular (non-SAML) custom resources with links to the various app pages - e.g. https://mail.google.com/a/yourdomain.com or https://drive.google.com/a/yourdomain.com, etc.

All types 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 part of this.