Migrating from OALA to OpenAthens in a federation

As support for OpenAthens LA is ending you will want to migrate to another solution. You have several options, but your easiest path is to migrate to hosted OpenAthens. and this guide covers how. The guide is tailored to users in the UK Access Management federation, but all federations will be similar.

If you are unclear or unsure, our service desk will be happy to help. They will also connect you to the right people if you are interested in arranging a consultancy which has options for on-site work and training.

Decisions to make first

The biggest decision is about your entityID. You can have a new entityID when you migrate or keep your existing one. Both have advantages:

	Keep same entityID	**Use a new entityID**
Advantages	Maintains the user IDs seen by publishers Publishers do not need to update your subscription settings No need to coordinate times with publishers	Completely fresh start Both can appear in the same federation at the same time
Disadvantages	EntityIDs must be unique within a federation so both old and new can't be in the same federation at the same time	Users appear to publishers with a different ID (per-user settings can be lost) All publishers must update their subscription records with your new details at the same time

Keeping the same entityID

The advantages are that you do not need to coordinate a change with all service providers, and it becomes possible to maintain the users' targetedIDs so that they do not lose personalisations such as saved searches or bookshelves.

The UK fed metadata is usually updated at 16:30 and after it changes to point your entityID at hosted OpenAthens there will be a period where the resources have not updated their cached copy of the federation metadata and will still to send users to OALA, so you will need to keep that running for a time to maintain access . How long will depend on your set of resources but most will pick up the change inside a day. Keeping an eye on the statistics reports in both OpenAthens and OALA will show you which, if any, resources are lagging and may need a reminder to update their copy of the metadata.

The following assumes you want to maintain the user IDs seen by publishers. If you don't, there are still advantages to keeping the same entityID but you can skip step 2.

Prerequisites

- The authentication store you are connecting to OpenAthens is the same one you were using with OALA and will be passing the same user identifier (if maintaining user IDs).
- You have access to the OpenAthens administration site
- You have access to the OALA administration console
- You have looked up your OpenAthens domain name (usually the same as your scope)

Process

1. Connect your local datastore to OpenAthens. There are several options (see: Connections). You will probably need help from your IT team for this bit.
    a. If you are using ADFS to replace an ActiveDirectory connection and were using objectSid as the user identifier there is an extra step, otherwise you just need to make sure that ADFS is sending the required attributes and you enter the claim names exactly.
2. Over and above the standard setup of your connection you will need to:
    a. Set the 'Unique user' attribute to be an attribute or claim containing the same value as the username field on OALA's authentication store tab
    b. Set the 'Salt value' to match the salt on the targetedID attribute(s) on the attributes tab
3. Contact our service desk and ask them to update your entityID in our systems if it is different from OALA
    a. The default method will have you appear in the OpenAthens federation. This is usually desirable for things like the redirector but can lead to some organisation discovery pages being inconsistent which login point they send the user to during the time between the changes happening in both federations. If you are affected and the period between updates will mean a significant impact on your users we can leave your entityID out of the OpenAthens federation until a point after the change.
4. Contact the UK federation and have them update your entity.

a. What they need you to send them is your entityID, the new 'endpoints' and new certificate

i. First go to your OpenAthens metadata page at https://login.openathens.net/saml/2/metadata-idp/YOUR_OPENATHENS_DOMAIN/c/ukfed

ii. Near the bottom you will find two lines that start with "<md:SingleSignOnService". The URLs on these lines are the 'endppoints' you need to copy

iii. The certificate is the block of text just above the endpoints between <ds:X509Certificate> and </ds:X509Certificate>

b. Send those, your entityID and the metadata address with a covering note to service@ukfederation.org.uk.

5. Update links

a. Your best bet is to update links to use the OpenAthens Redirector as this will (for compatible resources) allow you to simply add a target page to the end of a consistent prefix and will work out the rest in the background. If you are using a LMS or link resolver that has a proxy prefix feature, the redirector prefix can usually be inserted there.

b. In other cases:

i. Wafyless links that start with the SPs address will continue to work as is

ii. Wayfless links that started with OALA's SSO address should not need to exist any more, but if you have any that aren't compatible with the redirector you can replace the OALA SSO address with the ones in the endpoints you identified in step 4. You should try the one with /saml/2/ in it first.

Using a new entityID

Prerequisites

- You have access to the OpenAthens administration site
- You have looked up your OpenAthens domain name (usually the same as your scope)

Process

1. Connect your local datastore to OpenAthens. There are several options (see: Connections). You will probably need help from your IT team for this bit.

2. Contact our service desk and have them set the desired entityID value in our systems

3. Contact the UK federation and have them register the additional entity

a. What they need you to send them is your entityID, the 'endpoints' and certificate

i. First go to your OpenAthens metadata page at https://login.openathens.net/saml/2/metadata-idp/YOUR_OPENATHENS_DOMAIN/c/ukfed

ii. Near the bottom you will find two lines that start with "<md:SingleSignOnService". The URLs on those lines are the 'endppoints' you need to copy

iii. The certificate is the block of text just above the endpoints between <ds:X509Certificate> and </ds:X509Certificate>

b. Send those, your entityID and your metadata address with a covering note to service@ukfederation.org.uk.

4. Contact your resource providers and give them your new entityID (and scope) so that they can update your subscription details. Some may be able to support multiple entityIDs and scoprs at the same time but many will not so you should expect to have to coordinate a changeover date. At the arranged time, your old IdP will no longer work for access to resources and your new one will. Access may be spotty for the duration of the publishers changes.

5. Update links

a. Your best bet is to update links to use the OpenAthens Redirector as this will (for compatible resources) allow you to simply add a target page to the end of a consistent prefix and will work out the rest in the background. If you are using a LMS or link resolver that has a proxy prefix feature, the redirector prefix can usually be inserted there.

b. In other cases:

i. Wafyless links that start with the SPs address will continue to work as is

ii. Wayfless links that started with OALA's SSO address should not need to exist any more, but if you have any that aren't compatible with the redirector that you still need to use, you can replace the OALA SSO address with the ones in the endpoints you identified in step 4. You should try the one with /saml/2/ in it first.

Further configuration / equivalent functions

The items here are things you can do at any time during the migration and apply whatever you decide about entityIDs

Release policies

The essential difference is that in OpenAthens, release policies are only additive - i.e. you can't say 'if it's provider X do not release Y', they are all 'if it's provider X do release Y'.

The default policy releases targetedID, scopedAffiliation and entitlement. In most cases you will not need to add any additional policies, but if you do you search for the resource and tick the attributes that you want to release. You can change the NameID format on an SP by SP basis and even alias the attributes if the SP needs them called something else.

For details see:

- Attribute release

Mapping attributes

There are two considerations here. If you will want to release the attribute to a publisher, or use it in reporting, then you will need to map it to an attribute you have created via the schema editor. If you merely want to display the data in the interface then you can just make up a name.

For details see:

- Attribute mapping
- About schemas

'entitlement' values

The value pairs for these are baked into permission sets. Set it up there and assign to users on the permissions tab of your connection.

For details see:

- Federated attributes
- Permission sets
- Permission set rules

Statisitcs

Stats are aggregated on a handful of default attributes and any others you specify via the schema editor.

Default stats aggregations:

- Permission set
- Resource
- Organisation

Anything else you want, such as user ID, will need to be mapped to an attribute that is marked as reportable.

For details see:

- Reporting
- Schema editor

Additional service providers

If you want to connect to a SAML SP that isn't in a mutual federation - e.g. your VLE - you can create the connection via the resource catalogue.

Go to Resources > Catalogue > Custom tab > Add > SAML and upload the metadata. Once done you'll just need to set up the release policy.

For details see:

- Add and manage custom SAML resources

Anything else?

Because some publishers don't restrict access properly based on attributes there is an option to have us not send a response to a resource that isn't specified by permission sets assigned to the user. This is called restrictive mode and if you decide to use it you will need to ensure that all users get assigned an appropriate permission set and that those sets contain the relevant resources.

Do not turn it on until you are [fairly] sure you've allocated things correctly. The setting is at the bottom of the page under Preferences > Organisation.

For details see:

- Permission sets
- Catalogue
- Account preferences

Retiring OALA

Once the migration is complete, all publishers are sending users to the correct authentication point, and working as you'd like you can turn off OALA. Before you do, you might like to take copies of some of the files for historical stats, sentiment or 'just in case':

From the OALA admin console you might download a copy of your configuration. See How to backup and restore administration console databases

From the runtime(s) you might zip up the folder `/var/log/openathens` and store it somewhere. You might prefer to just export the stats database to CSV though. oala-categories.idx is probably the one you want:

```
>sqlite3 /var/log/openathens/oala-categories.idx
sqlite> .headers on
sqlite> .mode csv
sqlite> .output data.csv
sqlite> SELECT * FROM totals;
sqlite> .quit
```

Transfer the file with your favourite SFTP client.