Migrating from your own IdP

If you are moving from using your own IdP software (e.g. OpenAthens LA, or Shibboleth) in a federation to OpenAthens MD with a local connection, these are the things you need to know about and consider.

The main factor in how you would do this is whether or not you wanted to run both systems in parallel for any significant time.

Parallel running considerations

To run old and new in parallel you will need to register a second entityID with any federations you are part of and give it a different display name so your users can tell the difference. Using the same scope is ok.

Your resources will not grant the second entityID access until you ask them to. Some resources can support multiple entityIDs on a subscription, but some cannot - depending on your subscriptions, this may prevent you running two parallel systems as live, but it may be sufficient for a limited test.

The main concern with this method is usually that your users will present different targetedIDs to service providers when they are associated with the new entityID so will be seen as different people which means personalisations such as saved searches or alerts can be lost.

> If your users presenting different identifiers to service providers would be problematic, you may prefer to keep the same entityID (next section)
>
> If your users presenting different identifiers to service providers is not a major issue for you, then simply asking the the service providers to update your entityID and scope in their records to your new values can be a simple approach. You would need to contact all your service providers and coordinate a time.

Using the same entityID

It is possible to use the same entityID on both systems, but since federation metadata can only point to one of them at a time you cannot run both in parallel. 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.

When you transfer the entityID from your old IdP there will be a period where the resources have not updated their cached copy of the federation metadata and will try to send users to your old login. The time can vary by resource, but is usually no more than a day for most of them. As long as your old IdP is still running, users will still gain access although the login page they see might vary.

To migrate maintaining targetedID values

Prerequisites

- You are going to be re-using the same entityID with MD as you did with your old IdP
- You are using OpenAthens LA or Shibboleth as your existing IdP.
    - If Shibboleth you must have been using ComputedId as the targetedID hashing algorithm (this is the default)
- The authentication store you are connecting to OpenAthens is the same one you were using with your old IdP and will be passing the same user identifier.
- You have access to the OpenAthens administration site
- You have access to information from your old IdP's configuration settings
    - In OpenAthens LA, this would come from the administration console.
    - In Shibboleth, this would come from the `attribute-resolver.xml` file on the server.

Process

1. Contact our service desk and ask them to alter your entityID and scope on the system to the desired values as necessary.

    a. This will take effect immediately when changed so can affect access to resources if you have any people actively using OpenAthens accounts. You may wish to swap steps one and two.

2. Connect your local source to OpenAthens. (see: Connections)

3. If migrating from

    a. OpenAthens LA…
        i. Set the 'Unique user' attribute to be the same as the username field on your authentication store tab. This is usually sAMAccountName for Active Directory connections.
        ii. Set the 'Salt value' to match the salt on the targetedID attribute(s) on the attributes tab.

    b. Shibboleth... look up the following in your `attribute-resolver.xml` file and:
        i. Set the 'Unique user' attribute to be the same as the `sourceAttributeID`. This is usually `objectSid` for Active Directory connections and this will add a step if you are going to be using ADFS as your local source. See: objectSid and ADFS
        ii. Take everything between the quotes in the salt, including any brackets, and base64 encode it. Paste that base64 encoded value as the 'Salt value' in MD.

        Whilst this should work for any version of Shibboleth where you have used ComputedId as the targetedID generation method, and our service desk will always try to be helpful, they cannot support any third party software.

4. Contact federations

a. If you are only in the OpenAthens federation, this is automatic and you need do nothing more
b. If you are in the UK Access Management federation or InCommon, you will need to contact that federation and either register your new entity or update your existing entity with your new endpoints depending on whether or not you are maintaining personalisation. This is usually just a case of the registered management liaison emailing them - see below.
c. If you are keeping the same entityID, service providers will start to direct users to the new authentication point as they pick up the change from the metadata. This usually takes no more than a day.

5. If you have registered a new entityID...

    a. You will need to contact your resource providers and give them your new details. You will usually have to arrange a changeover date.
    b. At the arranged time, your old IdP will no longer work for access to resources and your new one will.
    c. You will have to update any WAYFless URLs you maintain with your new entityID (and for the older SAML1.1 type, your SSO address).

6. If you have kept the same entityID...

    a. You will need to update any of the older SAML 1.1 type of WAYFless URL you maintain with your new SSO address. SAML 2 WAYFless URLs are unaffected.

What to say to other federations

If you are updating an entity, you usually only need to specify your entityID and pass them your new IdP's metadata address.

The metadata address to pass is federation specific:

- UK federation: "https://login.openathens.net/saml/2/metadata-idp/DOMAIN/c/ukfed"
- InCommon: "https://login.openathens.net/saml/2/metadata-idp/DOMAIN/c/incommon"

...where DOMAIN is your OpenAthens domain (usually the same as your scope).

Your entityID and scope are displayed on the organisation summary page.

What to say to service providers if you are using a new entityID

You should just need to pass them your new entityID and scope as displayed on the organisation summary page and arrange a date.

Anything to watch out for?

Some service providers linked the user via a scoped version of targetedID. If your tests show that personalisation has been lost you can add a scoped version of targetedID to your release policy. Adding it on a per-resource basis is usually recommended, but it can be added to the global policy if necessary.