Attribute release

Path to function: ***Preferences > Attribute release***

This function allows you to release selected information about your users to third parties. You are responsible for ensuring you comply with all local rules and legislation relating to the release of this kind of data.

Jump to editing section

Where the schema editor can define additional attributes that are *available* for release, it is the attribute release section that decides which attributes *are* released to service providers.

This preferences page lets domain administrators set up two types of release policy:

Global

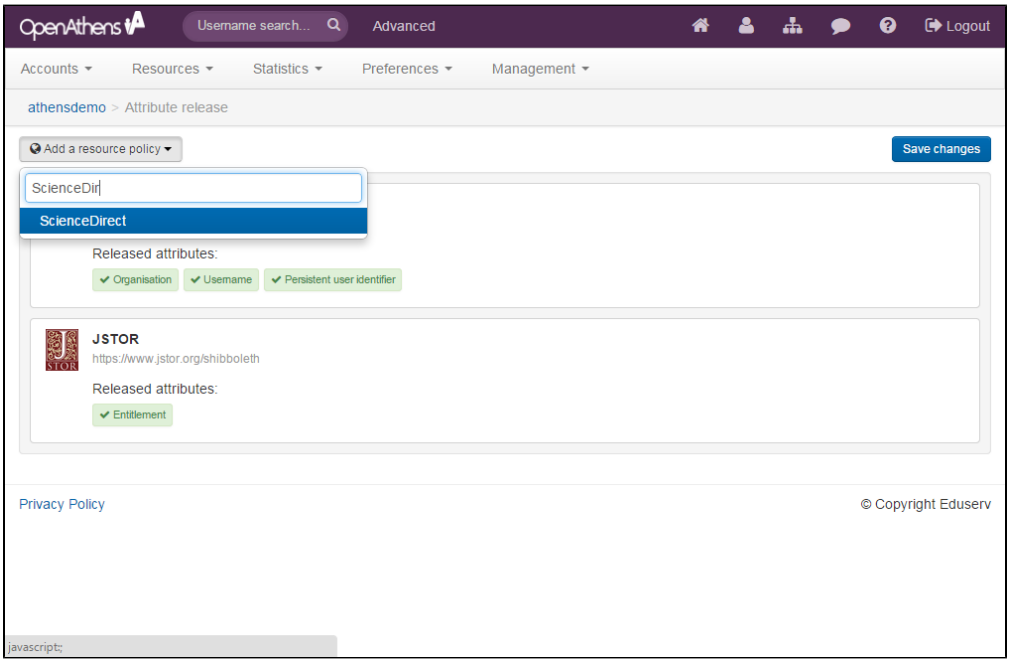
The global policy at the top of the list specifies which attributes are always released to any service provider. This is often enough by itself to satisfy the needs of most federated resources. You should not remove any of the default attributes from this policy.

Resource specific policies

Clicking the add button at the top of the page allows you to select a resource and then set a policy that releases additional attributes to that resource - for example if a specific resource required an email address or other identifier.

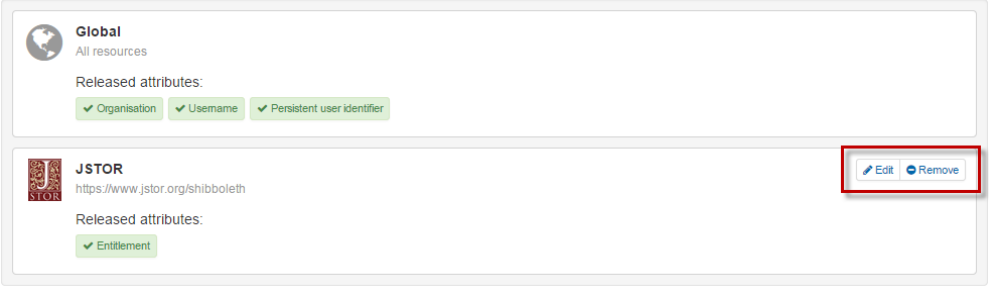
To add a resource, click the add button and start typing its name - the system will provide a short list to choose from that will get shorter as you continue to type. Once selected the resource will appear in edit mode in the list below the global policy; it will appear in its alphabetical position so you may have to scroll down.

The attributes released in a resource policy are in addition to those released by the global policy - they cannot restrict an attribute released via the global policy.

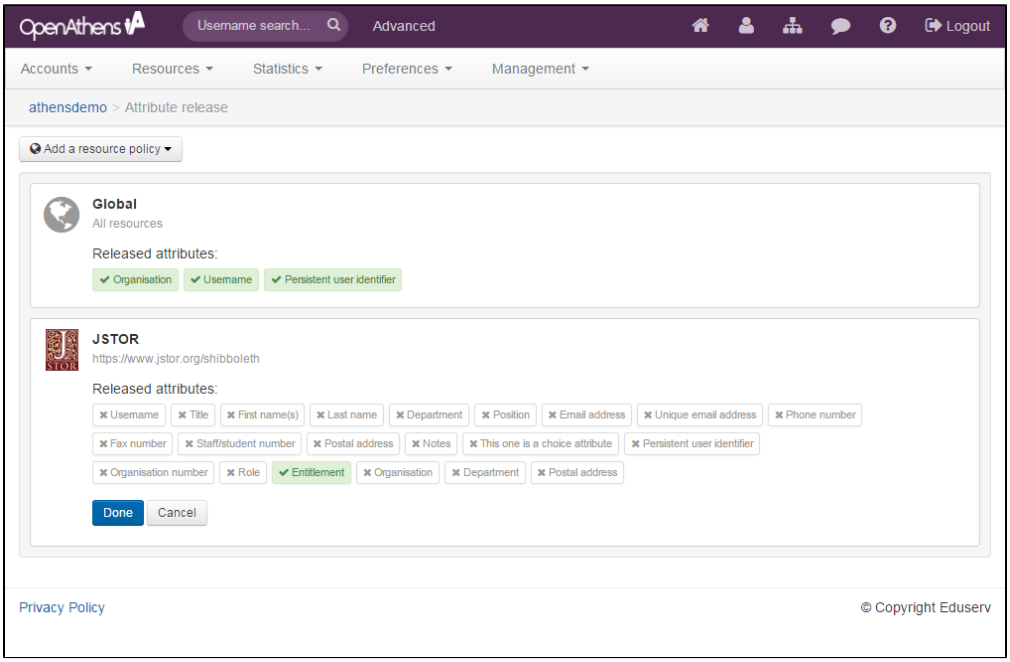


How to edit policies

As you mouse over policies you will see edit and remove buttons appear on the right:



When you click on edit you will see a list of all releasable attributes. The attributes that are highlighted in green and showing a tick mark are released to that resource (in addition to the global policy) and the grey ones with a cross are not.



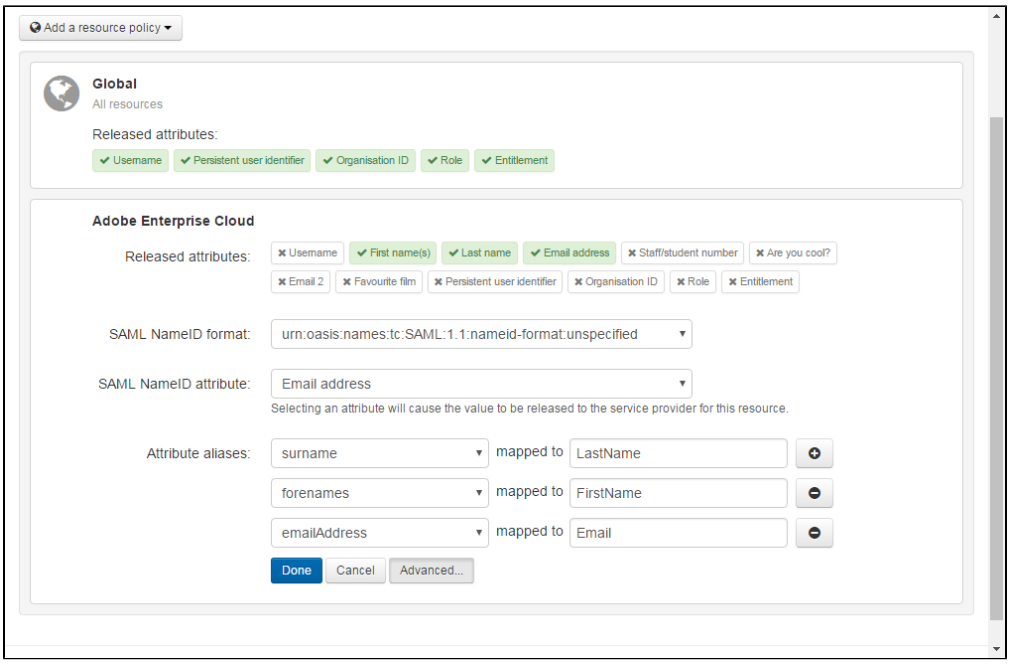
To change an attribute between unreleased and released, click on it.

The attributes display their display names here. To confirm the target name, hover over the attribute - it is this target name that would be used by any service provider you are releasing the attribute to such as *urn:oid:1.3.6.1.4.1.5923.1.1.1.1*.

Click done or cancel to exit the editor for that policy, keeping or discarding your changes. Once you click the save changes button at the top of the page the updated policies will go live immediately for new OpenAthens sessions (i.e. if you are testing this you will need to sign out and back in again to see the effect at resources or in debug mode).

Advanced

The advanced button visible in edit mode allows you to add attribute aliases - for example when you need to release an email address to a resource that is expecting it to have a specific name such as 'Email' rather than 'emailAddress'.



To set this up:

1. Add a per-resource policy if you do not already have one for the resource
2. Select Edit and tick the attributes that will be released
3. Click on advanced and select the attribute from the list in the box on the left
4. Enter the desired alias in the box on the right. Depending on the resource this can be case sensitive.
5. Use the plus button to add any other aliases to use for that resource, then click done and save.

In the same advanced dialogue you can also set a specific NameID attribute and format for the specified resource. This will not need to be used for federation resources, but some custom SAML resources may need this setting to be changed - e.g. G Suite requires a NameID format of emailAddress and a NameID attribute that contains the email address.

Recommendations

It can be tempting to set up a policy for each and every resource because that's how you assign them to permission sets, and whilst this approach can let you maintain very tight control over access we usually do not recommend it because it adds complexity, which in turn makes errors more likely. It would also make it more difficult to troubleshoot access problems should there be any.

The recommended approach in most cases is to set the global policy to release a couple of key attributes that satisfy most resources and only add resource policies for the [usually] small number of resources that expect more. You might then use restrictive mode to prevent access to resources that you had not specified in permission sets should you wish to maintain a tight control.

Personal attributes such as email address or real name, if being released at all, should generally be included in resource policies rather than the global policy.

Anything to watch out for?

Per resource policies cannot block the release of any attribute released by the global policy.

By default, all attributes in the global policy will be released to any service provider in the federation that the user tries to access. This can be curtailed if necessary by restrictive mode.

If you have mapped any local connection attributes to releasable schema attributes, then that data will also be released (or not) by policies you create here.

If the service provider in question only supports the old SAML 1.x standard then attributes are not transmitted quite as securely, so you may prefer not to pass data such as email addresses or real names.

If you are passing either the department or postalAddress attributes and both the account and the organisation have values set, both values will be sent.