Testing an IDP

Testing authentication

New for IDP 4.1: In order to test/verify your IDP's authentication configuration it's easiest to use the Hello world feature:

- Add the login name of the account you want to test authentication with to the AccessByAdminUser entry in conf/access-control.xml (and uncomment that section, of course)
- Reload the access control config, /opt/shibboleth-idp/bin/reload-service.sh -id shibboleth.
- Access /idp/profile/admin/hello on your IDP server.

Older systems (or those who disabled the Hello world module for whatever reason) will have to complete a few more steps in order to test authentication:

Provided you already have completed your metadata configuration by following our instructions you can test your authentication configuration with a web browser using IDP-initiated SSO URLs. While the details for this (as always) are fully documented in the Shibboleth Wiki it should suffice to know that the URL needs to look like this:


Where "YOUR-PUBLIC-IDP-HOSTNAME" above needs to be replaced with just that, e.g. "weblogin.example.edu". This should then create a Shibboleth IDP-specific authentication request to your IDP which then should lead to your IDP's login page being displayed. Entering correct (and also incorrect) credentials can then be used to determine whether authentication works as desired.

Testing the attribute resolver and filter

Using the "Hello world" endpoint (see above) you can also test the attribute resolver (and the attribute registry) in isolation, without the need for a Service Provider.

Command Line Interface

Provided you already have completed our metadata configuration instructions you can test both your attribute resolver and attribute release from the command line without the need for a "Test SP" that shows you what it recived successfully. This greatly accelerates configuration verification of your IDP so do make use of this (with before/after tests) when changing e.g. your resolver or filter configuration. (You could also use this on a test machine to verify the changed configuration works as expected before transferring the tested config to the production server.)

The official documentation of course has all the details, but commonly all you need is to run the following command on our IDP server:

/opt/shibboleth-idp/bin/aacli.sh --saml2 -n SOME_USERID -r https://test-sp.aco.net/shibboleth

Where "SOME_USERID" above needs to be replaced with the userid/login name people would enter as part of authenticating to your IDP. Then the attributes, their values as well as any NameIDs that would be sent to the SP identified by its entityID -- in the above example that would be the eduID.at SAML Demo SP -- will be shown, in XML the way it would be sent in a SAML Assertion (after encrypting and encoding the data to the SP named as recipient, of course). You could use this command without the --saml2 parameter but the simpler output you get that way may hide some of the details that are relevant when debugging attribute release issues. So it may be best to always use the --saml2 output to learn how the SAML is supposed to look like.

Note that no data is sent to the specified SP using that method: This command simply provides an answer to the question "What attributes (and NameIDs) -- if any -- would the IDP send for account X to service Y using the currently running configuration?"

Also note that the IDP will use the currently running/loaded configuration for this, not anything you have edited/changed since the IDP was started or reloaded. I.e., the aacli cannot be used to test configuration changes before applying them to the running IDP. (If that's what you need you would have to use a test IDP installation on a different machine.)

Test Service Provider

ACOnet also operates the eduID.at Demo SP for full end-to-end testing involving your web browser, authentication, attribute lookup and filtering, signing (and signature verification, at the SP) encryption (and decryption, at the SP), etc. This SAML SP knows all eduID.at IDPs and so is available to anyone having access to an IDP registered in eduID.at.
Once your IDP has been registered and published in eduID.at metadata using that specific URL is no longer necessary (though it will continue to work) – you can then simply select your IDP from the IDP Discovery Services offered at the eduID.at Demo SP.

Testing scalable attribute release

Those (also) participating in eduGAIN/Interfederation will want to know how well their IDP works with Service Providers registered in other federations, i.e., what attributes it’ll send to what SPs and why:

“The eduGAIN Attribute Release Check allows testing whether the Identity Provider of an organisation participating in eduGAIN properly releases user attributes to eduGAIN services.”

This will illustrate the good use (or lack thereof) you’ve made of the Service Categories defined by the global academic community to streamline access to academic resources.

IDPs following our documentation and recommendations should expect to see “A+” for all tests that receive a score (as per end of year 2022). I.e., if you’re seeing some other result you’re not following our documentation and recommendations and the community your IDP is intended to serve will likely be missing out.

Testing specific services

You should also test how your IDP interoperates with selected services important to our academic community, specifically:

- To ensure continued access to the Erasmus+ services perform the MyAcademicID Attribute Release Test for students and non-students.
- The InAcademia affiliation test ensures your students (and/or faculty, staff and other members) can get their discounts at selected online retailers without having to hand over loads of personal data to so-called student discount platforms.