eduGAIN Access Check

Federation operators and eduGAIN experts are frequently asked how to test access to a production federated service. A simple login test to a federated service requires a federated account at an organisation that is part of the federation/eduGAIN. However, commercial service operators normally don't have federated accounts in a national federation and eduGAIN. And even if they had a single account of their own or if they asked a real-world user to test, this would not be sufficient to thouroughly test federated login with multiple identities and different sets of attributes.

Setting up a SAML Identity Provider (IdP) and using it to test its Service Provider (SP) would be ideal but is non-trivial and therefore in most cases too much effort. Using self-registration IdPs (e.g. https://openidp.feide.no/) and configuring them bilaterally with their Service Provider (SP) might be sufficient for development but as these IdPs are not part of eduGAIN, they don't allow federated login under real conditions from an eduGAIN IdP. Also, self-registration IdPs usually don't allow certain attributes (e.g. affiliation) to be set.

The eduGAIN Access Check solves most of the forementioned issues because it provides SP operators an easy way to test federated login for their eduGAIN service with test identities that have different attribute profiles.

Benefits of the eduGAIN Access Check

The eduGAIN Access Check allows SP administrators to ensure proper functioning of their services within eduGAIN. It is especially useful for services not hosted by an R&E institution, because they can't use their own IdP to login and test their production eduGAIN-enabled service. Setting up an IdP on their own would require considerable efforts on their part.

The eduGAIN Access Check provides realistic user profiles (e.g. including non-ascii characters, typical attributes) to help SP administrators to improve and adapt their eduGAIN-enabled services to the constraints of variable attribute release in an international context. In particular, the eduGAIN Access Check makes the SP operators aware that:

1. different eduGAIN IdPs will release varying set of attributes
2. the vocabulary and semantics of some attributes (i.e. eduPersonAffiliation) differ from federation to federation

SAML2 entity categories (GéANT Data Protection Code of Conduct, REFEDS Research & Scholarship) support for attribute release management is a non-trivial concept within eduGAIN. The eduGAIN Access Check releases a reasonable set of attributes to SPs, depending on the entity categories they belong to. This should encourage SP administrators to follow the eduGAIN guidelines and facilitate the use of entity categories.

Frequently asked questions

I run a SAML-enabled service. How can I use the eduGAIN Access Check?

Your Service Provider first needs to be registered in eduGAIN metadata. Therefore, you should contact your nearest federation operators (please have a look at the list of eduGAIN member federations) to find out about the local process to join eduGAIN.

Once your SP's metadata is included into eduGAIN, you can start creating test accounts. Before you obtain the test accounts, it is checked that you are a legitimate administrator of your SP. This is achieved via an email challenge sent to the contact address for the Service Provider.

To use the test accounts, initiate a login at your SP. On the Discovery Service, select "eduGAIN Access Check" as your Identity Provider and then use the credentials of one of the created test accounts. Once authenticated, the eduGAIN Access Check IdP will send your SP a realistic set of user attributes. This allows you to validate that your service behaves as expected.

How long can I use the eduGAIN Access Check test accounts?

Test accounts expire automatically after a few days. However you can ask for new test accounts, via the same process, if you still need it.

How can I provide the eduGAIN Access Check within my federation?

The code of the eduGAIN Access Check Account manager is published as open source. It's available at: https://code.geant.net/stash/projects/GN4SA2T2/repos/edugain-access-check---account-manager/browse. Feel free to install it to run you own instance of the service.

If national federations don't want to have their own service but still want the eduGAIN Access Check as a service in their federation to be use by all their SPs, they can request that. The eduGAIN Access Check then would be configured to also load the metadata of that federation in addition to eduGAIN. Vice versa, the national federation then would have to include the metadata of the eduGAIN Access Check IdP in their local federation's metadata.

How does this Identity Provider compare with test identity providers and guest identity providers?

Test identity providers provide test accounts, with well-known accounts credentials. If such a test IdP is registered in eduGAIN, it allows access to any registered eduGAIN SP with these test accounts, unless the test IdP is filtered out, either at the SP level or at national federation level.

Guest or self-registration identity providers typically allow all users with a valid email address to create an account and access federated services with it. This is mainly for users who don't/can't have an account at an institutional IdP. These guest IdP rely on mail address verification (based on a challenge for instance) as a provisioning method but any other attribute is either self-provided by the user (unknown quality) or static. Therefore, tis type of IdP provides generally provides low quality attributes about the users (name, email, user identifier) and typically cannot release user attributes carrying privileges because data is self-provided by the user. Guest or self-registration Identity Provider therefore are generally not recommended to be part of eduGAIN.

Unlike a test IdP, eduGAIN Access Check test accounts credentials are provided to the requestor only.
Unlike a guest or self-registration IdP, the eduGAIN Access Check test accounts creation is a restricted feature; you need to proove that you are administrator of an eduGAIN production SP to use it.
Unlike for a standard IdP, the eduGAIN Access Check test accounts can be used to access a single SP. If you request test accounts as admin of SP A; these test accounts won't allow accessing any other SP than A.

How is it ensured that users can only test their own service?

The eduGAIN Access Check service exclusively allows creating test accounts for users who can receive challenge emails for contact email addresses listed in the eduGAIN metadata for a particular Service Provider. The test accounts can be used exclusively to access a single SP (for which a user proofed that he is administrator for). Authentication requests for other SPs are rejected.

What prevents the eduGAIN Access Check from being used to impersonate real eduGAIN users?

The attributes that are typically needed for user identification have a hard-coded domain name ("@access-check.edugain.org") set. Therefore, they cannot be changed unless the host is hacked, which could happen of course to any Identity Provider. The eduGAIN Access Check also has the Shibboleth metadata scope extension set to "access-check.edugain.org" in its published metadata. Therefore, an SP with enabled scope check would not accept for example an eduPersonPrincipalName with a different scope.