How to Join eduGAIN as Service Provider

Introduction

This page is for service providers who want to offer their SAML-enabled services to users and institutions worldwide. Thanks to the eduGAIN, services will be available to the users of identity federations of more than 60 countries around the world. Joining a single eduGAIN member federation allows the users from all other eduGAIN member federations to access your service. This minimizes the technical and contractual work considerably. If you are interested in a very brief introduction to eduGAIN, please have a look at the About eduGAIN web page.

So, if you're a service operator (provider of resources to the academic and research community) and are looking for a way to allow higher education users to authenticate to your service via federated access, you find on this page the relevant steps that describe how a service can be integrated with eduGAIN as a SAML Service Provider.

The rest of this page's target audience is IT service administrators of organizations or communities. Examples of organizations and communities that typically are interested to operate a service in eduGAIN are:

- research communities (i.e. international research projects)
- e-journal content providers (i.e. publishers)
- cloud service providers (i.e. suppliers of research projects)

Once you have read this page and followed the instructions, you will have deployed a SAML2.0 compliant Service Provider and published it in eduGAIN. This means that a few million higher education users (students, university staff and faculty, researchers) will be able to able to access to your services using their home institutions account, depending on the access control rules you have defined.

Prerequisites

Before attempting to follow the steps below, which explain how to deploy and register a SAML Service Provider with eduGAIN from scratch, it is recommended to first get familiar with some key concepts of federated identity management, the basis of eduGAIN and all SAML identity federations. A comprehensive overview of material that you might want to have a look at is available at the AARC Federations 101 page.

If you have little time and prefer audio/visual documentation, watch the 4 minute movie "How to benefit from interfederating through eduGAIN".

If you want to see and try federated login in action, have a look at SWITCH's AAI Demo.

General eduGAIN information

eduGAIN is an interfederation service developed within the GÉANT Project - a major collaboration between European national research and education network (NREN) organisations and the European Union.

An (identity) federation is a group of organisations that agree on a set of common standards, policies and practices to issue and accept identity assertions. Identity assertions are issued by an Identity Provider (IdP) that authenticates a user (e.g. by password). The Identity assertions then are consumed by Service Provider (SP), which uses the attributes of that assertion to perform access control and to provide the user attributes to the web applications it protects.

eduGAIN as interfederation service basically interconnects academic identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN thus enables the trustworthy exchange of information related to identity, authentication and authorisation (AAI) by coordinating the federations' technical infrastructures and providing a policy framework that controls this information exchange.

About 40 national federations currently take part in eduGAIN. This amounts to over 2200 Identity Providers worldwide, allowing their users federated access to over 1000 Service Providers offering their services in eduGAIN.

Some **key features** of eduGAIN can be summarized below:

- Enables **trustworthy exchange of identity information** between federations without many bilateral agreements
- **Reduces the costs** of developing and operating services
- **Improves the security** and end-user experience of services
- Enables service providers to greatly **expand their user base**
- Enables identity providers to increase the number of services available to their users

Joining eduGAIN

The publication in an eduGAIN member federation, for a Service Provider, allows reaching students, researchers and staff of worldwide higher education institutions without the technical and administrative inconveniences of maintaining and protecting repositories of user credentials. This is because authentication is always handled directly at and by the user's home Identity Provider, while the Service Provider only has to deal with user Authorization. In Identity and Access Management, authentication is the process of confirming a user's identity, usually by verifying the knowledge of a set of credentials (username, password). Authorization is the process of determining the access rights an authenticated user is eligible for. In eduGAIN terms, this would mean that a user accesses the Service Provider with an assertion of his identity and the Service Provider trusts that assertion because it comes from a trusted relying party, but it is always the Service Provider that decides to which parts of the service this authenticated user should have access.

Enabling a service for eduGAIN login is accomplished by joining an existing eduGAIN member federation and registering a Service Provider with this federation. The member federation then, following its own procedures, exposes the Service Provider to the rest of the eduGAIN federations and their entities.

Which (eduGAIN) federation to join

Joining eduGAIN means joining an eduGAIN member federation. But which one to join? There is no strict rule which federation to join. But one reasonable option should be to contact the national federation of the country where the Service Provider's organisation is located or where the service is geographically operated (i.e. where its operators are located). This offers multiple benefits, such as ease of collaboration and access to documentation because of common shared native language, shared groups of interested prospective users, etc.

Please find a list of eduGAIN member federations with contacts and joining policies on the eduGAIN Technical site:

- https://technical.edugain.org/status

If your service is located in a country that has an identity federation that is already an eduGAIN member, please follow their guide or get in touch with them though the contact addresses. As explained above, a service can join eduGAIN via any eduGAIN member federation. To become available as an eduGAIN service, a service only has to join one eduGAIN member federation.

If your service is located in a country without an identity federation, or where the federation is not already an eduGAIN member, please contact the eduGAIN Support at support@edugain.org.

Is that Service Provider already in eduGAIN?

Consider also that in some cases a service is already available via eduGAIN without you knowing it. This is sometime the case for publisher services that in pre-eduGAIN times were often registered with many national federations. When one of those national federations joined eduGAIN and exported their services, they become availabel through eduGAIN as well. To verify if your service is already exported to eduGAIN look it up in the eduGAIN Entity Database:

- https://technical.edugain.org/entities

Is that Identity Provider already in eduGAIN?

All that then remains to do is to check if the Identity Providers (IdP) of your target user's organisation are also in eduGAIN, so as for the service provider you can look it up in the eduGAIN Entity Database:

- https://technical.edugain.org/entities

If you are unsure about the exact name of the entity, you can also look up the domain name of the organisation through the eduGAIN isFederated Check.

Installation and Configuration

Guides

Most eduGAIN member federations publish guides on how to install and configure a Service Provider, please refer to the respective nation identity federation documentation sites for more details (https://technical.edugain.org/status).

Attribute Availability

There are not recommendations from eduGAIN as to which attributes that eduGAIN Identity Provider should be able to release about their users. Attributes are also generally not released by default. Typically, Identity Providers only release those attributes that are requested (as in the SP's metadata) by a Service Provider.

Please think carefully which attributes you might need in your application. Then set the Requested Attributes for your SP's metadata accordingly. It might be helpful to read the recommendations which attributes to request as Service Provider.

Discovery Service

In order to provide the best experience possible for your users, following the best practices described in https://discovery.refeds.org/ is highly recommended.

Support for Code of Conduct and R&S Entity Categories

Entity categories allow to categorize entities (Service Providers and Identity Providers) in metadata. If an entity in metadata contains the value representing an entity category, this means that the entity typically meets this category's requirements.

Entity categories can be defined by any federation. However, in the context of eduGAIN, only the following two entity categories have an effect on a global level because the eduGAIN community has agreed to support them. Both affect the attribute release at Identity Providers:

- **Data Protection Code of Conduct (CoCo)**
  The Data Protection Code of Conduct (CoCo) basically is a promise by the Service Provider to follow the EU data protection law. It gives Identity Providers the sometimes necessary confidence to safely release release attributes to Service Providers that are operated in the EU. Detailed instructions on how your Service Provider can support the Code of Conduct can be found here. Basically, it means writing a data privacy statement (examples are references on the wiki page) and then adding a special entity category value to the metadata of your SP.
- **REFEDS Research and Scholarship (R&S)**
  In the same manner, the REFEDS Research and Scholarship (R&S) Entity Category is used to support the release of attributes to Service Providers meeting a set of predefined requirements. Basically, if you are registering a Service Provider for a research community, then you are likely to get the R&S entity category if you request it. Details about supporting REFEDS Research and Scholarship can be found here.

If possible it is highly recommended for your SP to support both, the GÉANT Data Protection Code of Conduct and REFEDS Research & Scholarship entity categories, as they are a trust establishing factor that will maximize the chance that Identity Providers release all the attributes requested by your Service Provider.

SP Metadata

To register the Service Provider (SP) with a federation, one typically has to provide its SAML2 metadata to the federation operator. If you don't have metadata about your SP yet, you might need to generate/compose it first. Shibboleth can generate SAML2 metadata about itself, just try accessing https://your.host.org/Shibboleth.sso/Metadata

SimpleSAML PHP has a similar feature. Just open the URL https://your.host.org/simplesaml/module.php/saml/sp/metadata.php/default-sp

In both cases, metadata only contains technical information. You should enrich metadata with the non-technical information (e.g. technical contact, name, description) following this example.