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 in several countries. Thanks to the advantages of eduGAIN, such services can connected to the identity federations of more than 50 countries around the world with scalable efforts. Joining a single eduGAIN member federation allows the users from all other eduGAIN member federations to potentially also access your service (if you allow that). This minimizes the technical and contractual work considerably. If you are interested in a verb brief introduction of eduGAIN in form of a video, 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.

This rest of this page's target audience is technical people (i.e. administrators) of organizations or communities that operate the service. 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 its 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) can - depending on the access control rules you define - get access to your services using their home institutions account.

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 don't have much time and prefer audio/visual documentation, you might want to watch the 4 minute movie "How to benefit from interfederating through eduGAIN".

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

Before you Begin

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 participate in eduGAIN. This amounts to more than 2200 Identity Providers worldwide allowing their users federated access to more than 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

Limitations

While eduGAIN provides many benefits for service operators, organisations and users, there also are a few limitations that a service operator should be aware of.

Joining eduGAIN

The publication in eduGAIN, for a Service Provider allows reaching a large audience of higher education users (students, researchers, staff of higher education institutions) without the technical and administrative difficulties 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 participating 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.

The list of currently participating national federations in eduGAIN and the contact details of their technical and administrative representatives can be found here

Please find below a list of eduGAIN member federations, a link to the joining instructions (if any) and a contact email address:

Country	Contact Address	Joining Instructions
Armenia	admin@afire.asnet.am	Not Available
Austria	eduid@aco.net	https://wiki.univie.ac.at/display/federation/Joining
Belgium	edugain@belnet.be	http://federation.belnet.be/node/12 http://federation.belnet.be/node/27
Brazil	operacao@cafe.rnp.br	https://www.rnp.br/en/services/advanced-services/cafe
Canada	caf@canarie.ca	http://www.canarie.ca/identity/join/
Chile	cofre@reuna.cl	http://cofre.reuna.cl/index.php/en/joining-sp
Colombia	tecnico@renata.edu.co	Not Available
Croatia	team@aaiedu.hr	http://www.aaiedu.hr/za-davatelje-usluga/registar-resursa?language=hr
Czech Republic	eduid-admin@eduid.cz	http://www.eduid.cz/en/join#step-by-step_guide
Denmark	eduGAIN-operations@wayf.dk	http://wayf.dk/en/services/how-to-get-my-service-connected http://wayf.dk/en/services/edugain
Ecuador	info@cedia.org.ec	Not Available
Estonia	eenet@eenet.ee	http://taat.edu.ee/main/teenusepakkujale/kuidas-liituda/
Finland	haka@csc.fi	https://confluence.csc.fi/display/HAKA/Joining+and+registrations https://confluence.csc.fi/pages/viewpage.action?pageId=39066043
France	fed-contact@listes.renater.fr	https://services.renater.fr/federation/en/sp

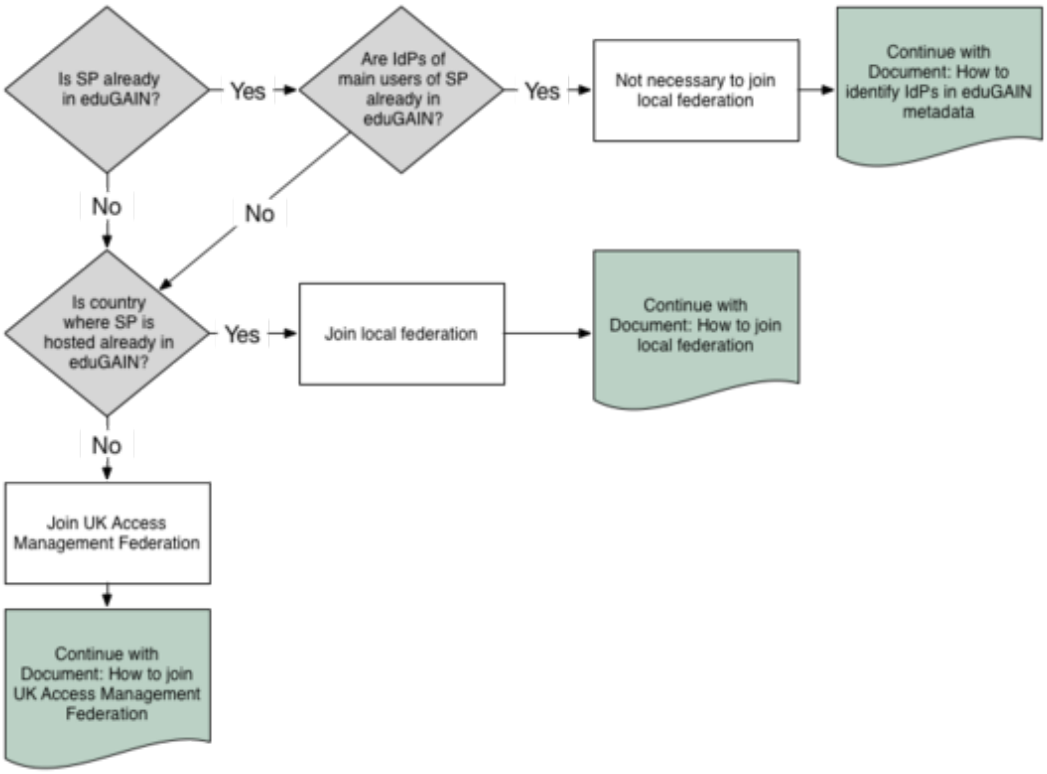
Georgia	gif-support@grena.ge	http://gif.grena.ge/eng/main/index/13
Germany	edugain@dfn.de	https://www.aai.dfn.de/en/join/ and https://wiki.aai.dfn.de/de:edugain
Greece	helpdesk@grnet.gr	Not Available
Hungary	aai@niif.hu	http://www.eduid.hu/hu/reszletek/
Ireland	noc-middleware@heanet.ie	Not Available
Israel	info@iif.iucc.ac.il	https://iif.iucc.ac.il/join/
Italy	idem-help@garr.it	https://www.idem.garr.it/en/join
Italy /International	credentials-admin@ct.infn.it	http://gridp.garr.it/documentation.html
Japan	gakunin-office@nii.ac.jp	https://www.gakunin.jp/en-Join/
Latvia	laife-admin@lanet.lv	Not Available
Lithuania	fedi@litnet.lt	http://fedi.litnet.lt/en/rps http://fedi.litnet.lt/en/edugain
Luxembourg	admin@restena.lu	http://www.eduid.lu/en/EN-participate.html
Moldova	leaf@renam.md	http://federations.renam.md/index.php?menu=join
Norway	support@feide.no	https://www.feide.no/service-providers
Poland	kontakt@aai.pionier.net.pl	https://aai.pionier.net.pl/en/index.php?page=rps
Portugal	noc@fccn.pt	https://www.fccn.pt/en/services/connectivity-and-infrastructure/rctsaai-federation/#!/en/services/connectivity-and-infrastructure/rctsaai-federation/service-recipients/
Slovenia	aaa-podpora@arnes.si	https://aai.arnes.si/
South Africa	safire@tenet.ac.za	https://safire.ac.za/participants/sp/join/
Spain	siri@rediris.es	http://www.rediris.es/sir/docs/howto-sp.html
Sweden	operations@swamid.se	https://www.sunet.se/swamid/
Switzerland	aai@switch.ch	https://www.switch.ch/aai/join/ https://www.switch.ch/aai/support/documents/interfederation/
The Netherlands	support@surfconext.nl	https://www.surf.nl/en/services-and-products/surfconext/index.html https://wiki.surfnet.nl/display/surfconextdev/Documentation+for+Service+Providers
U.S.	admin@incommon.org	https://www.incommon.org/join.html
Ukraine	peano@uran.ua	http://www.peano.uran.ua/~eng/frames.htm
United Kingdom	service@ukfederation.org.uk	http://www.ukfederation.org.uk/content/Documents/JoinFederation http://www.ukfederation.org.uk/content/Documents/EduGAINParticipation

If you have a relationship to one of the above eduGAIN member federations, please follow their guide or get in touch with them using the given contact address. As explained above, a service can join eduGAIN via any eduGAIN member federation that accepts it. In order to become available as an eduGAIN service, a service only has to join one single eduGAIN member federation.

If you have no relationship yet to one of the eduGAIN member federations and is also not located in a country where an eduGAIN member federation is deployed, it is recommended to join the UK Access Management Federation and register the service there. The UK Access Management Federation (UKAMF), as the largest academic identity federation in the world, is the “federation of last resort” for eduGAIN.

In some cases a service is already available via eduGAIN without you knowing it. This is often the case for publisher services that were (in pre-eduGAIN times) often registered with many national federations. Therefore, some services are already published in eduGAIN. If your service already supports SAML login (i.e it uses a SAML Service Provider), it is recommended to first check that the Service Provider (SP) is not yet in eduGAIN. This can be checked by searching for the service's domain name on the REFEDS MET service, which contains a complete lest of all federated services worldwide. If MET finds an entry for your service and if it lists eduGAIN as one of the federations that includes your service's metadata, you might not have to register the service again. All that then remains to do is to check if the Identity Providers (IdP) of your target user's organisation are also in eduGAIN. This can be check with the domain names of these organisations and the eduGAIN isFederated Check. If the majority of organisations of your service's target group is federated but not in eduGAIN, it still might make sense in the short term to join a local federation .

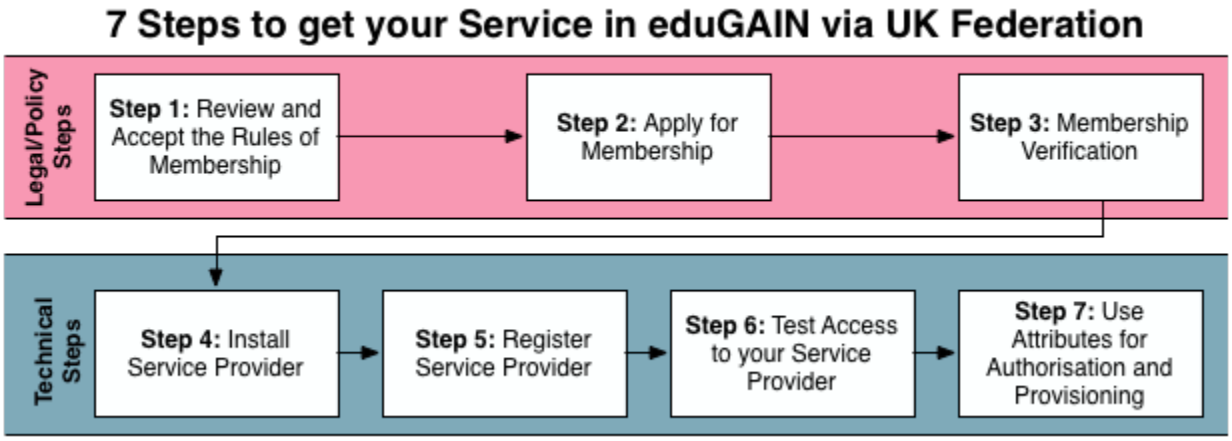
The above cases are summarized in the following graphic.



The rest of this page describes the process of joining eduGAIN by joining the UK Access Management Federation. So, please only continue reading if you have no affiliation with one of the above eduGAIN member federation and if you therefore want to register the service with the UK Access Management Federation.

Instructions

This chapter offers detailed instructions on how a service can participate as a SAML Service Provider in eduGAIN by joining the UK Access Management Federation. There are basically two parts in this process: A legal (steps 1-3) and a technical part (step 4-7). The diagram below provides a brief overview, followed by more detailed instructions.



Step-by-Step Guide

Step 1: Review and Accept the Rules of Membership

Before becoming a member in the UK Access Management Federation and thus also eduGAIN, a Service Provider needs to review and accept the Rules of Membership for UKAMF, as published at http://ukfederation.org.uk/content/Documents/FedDocs

This document basically lists your rights and duties of offering a service in the UK Access Management federation and implicitly also eduGAIN.

Step 2: Apply for Membership

In this step, the organisation that operates the service formally requests to join the UK Access Management federation using the procedure described on the “Applying for Membership” page.

Requests to join the UK Access Management Federation must be signed by a senior officer of the organisation who is authorised to bind the organisation to the federation’s Rules of Membership. This person is then given the role of Executive Liaison for the organisation. An example letter of application is provided. Please also read through the rest of the page above before sending in your letter of application.

The application must be in writing, on the organisation’s letterhead, and sent to the UK Access Management Federation operator at the following mail address :

```
UK Access Management Federation Operator
Jisc Collections and Janet Limited
Ground Floor
Brettenham House
5 Lancaster Place
London
WC2E 7EN
```

The application must contain the following information:

- The name, job title and email address of the Executive Liaison, who is the signatory of the letter.
- The full name and postal address of the organisation (if a company, these should be the legal name and the company's registered address).
- A statement that the organisation agrees to be bound by the federation’s Rules of Membership, as published on the federation website.
- The name and contact details of one or more Management Liaisons authorised to make registration requests. In most cases, each Management Liaison will be an officer of the organisation itself, responsible to the Executive Liaison.

Step 3: Membership Verification

As described on the Member Verification page, the operator of the UK Access Management federation then will contact the individuals named in the letter of application (Executive Liaison, Management Liaison(s)) to confirm their email addresses. Named contacts should ensure that they respond promptly.

This is a very important step in order to process your registration request so please make sure that the contact details are correct and that the delegated persons are notified about the required actions in advance.

Step 4: Install Service Provider

Now that the registration application is under way, you might want to install and configure a Service Provider implementation, compatible with the SAML 2.0 specification. The two most popular implementations are:

- Shibboleth Service Provider, which is implemented and maintained by the Shibboleth Consortium. It's the most common and popular SAML implementation in eduGAIN and it also includes most features relevant for eduGAIN. Therefore, this is generally the recommended SAML implementation to use. It works very well with Apache and IIS as web server. It requires root access because it requires the mod_shib web server module.
- SimpleSAMLphp, which is implemented and maintained by Uninett. This PHP implementation of SAML is recommended only if PHP is already used. It does not require root access but to make use of federated login requires code changes in a PHP application.

Please read section 4.2 (Installation & Configuration), which contains detailed instructions for the installation and necessary configuration of a Service Provider, using one of the aforementioned implementations. Also make sure that, once installed, the Service Provider is tested using the SAML implementations sanity checks (e.g. for Shibboleth running "shibd -t" on linux) to ensure that the software was correctly installed. Ideally, the Service Provider is also tested against a SAML2 Identity Provider to ensure that it was configured correctly.

Note: It is not recommended to try creating an own SAML implementation. SAML is a very complex standard and trying to come up with something on your own, most certainly will cause interoperability issues. Generally, eduGAIN's Web SSO profile requires a SAML Service Provider to support the SAML2int profile.

Step 5: Register Service Provider

Once the Service Provider software is installed, configured (see section 4.2) and functional, the next step is to register the Service Provider with the UKAMF federation.

Before completing the following form, please also read the section 4.2.4 about SAML2 metadata and how to generate/compose it for your Service Provider. Then provide the request data and submit the form:

The submitted information will be validated against a predefined set of rules upon submission. It then will be submitted to the UKAMF operations team so that the Service Provider's metadata can be published in the federations metadata and published in the UKAMF's metadata export to eduGAIN. It can take from a few hours up to 1 day until your SP's metadata is published in eduGAIN.

Upon successful publication your Management Liaison will be notified and your Service Provider will be available as a service in the UK Access Management Federation and eduGAIN.

Step 6: Test Access to your Service Provider

After your Service Provider is registered, you are then welcome to test the functionality (i.e. federated login) yourselves. Unless you have an account at an eduGAIN Identity Provider, you can use the eduGAIN Access Check Service, available in https://access-check.edugain.org This service allows you to test federated login to your own service using a few predefined test identities.

What you should check is if your Service Provider receives the attributes it requests.

Step 7: Use Attributes for Authorization and Provisioning

Once the attributes are available at the SP, they can be used for Access Control or they can be used within your web application. How to do that is for example described on the Shibboleth Access Control example in the Shibboleth wiki. A simple Apache rule like the following would allow only students to access a particular directory of your application:

```
AuthType shibboleth
ShibRequestSetting requireSession true
Require shib-attr affiliation student
```

Attributes are typically also used to provision an account in web applications (i.e. create a user record in the database). To use attributes within a web application protected by Shibboleth, simply read them from the web server environment (where you also would read the REMOTE_USER variable from). For example with:

```
Java: request.getHeader("mail")
```

How to integrate SimpleSAML PHP with your PHP application is described on the SimpleSAML PHP Integration page.

Installation and Configuration

Guides

UKAMF's documentation offers an extensive section on how to install and configure a Service Provider.

- For a Shibboleth Service Provider please refer to their instructions provided in: http://www.ukfederation.org.uk/content/Documents/Setup2SP

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 before submitting the metadata in section 4.1 Step 5. 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.

Post Joining

Find below a few useful links for successfully operating and using a Service Provider.

Operation best practices

This section consists of a list of guides compiled by federations participating in eduGAIN that would prove useful in operating your Service Provider.

- **Shibboleth SP Access Control Rules:**
  Examples of how to create access control rules with Apache and Shibboleth
  https://www.switch.ch/aai/guides/sp/access-rules/
- **Best Current Practices for operating a Service Provider:**
  This was written specifically for the SWITCHaai federation but most recommendations are generic
  https://www.switch.ch/aai/docs/bcp/sp-latest.html

Maintenance

This section consists of a list of guides compiled by federations participating in eduGAIN that would assist with the maintenance of your Service Provider after it is put in production.

- **Shibboleth SP Certificate Rollover Guide:**
  Explains how to renew a SAML certificate for an SP without service interruptions due to a metadata propagation delay
  https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPMultipleCredentials#NativeSPMultipleCredentials-KeyRollover