How to test an eduGAIN Identity Provider

How to check if your Identity Provider is eduGAIN-ready

An eduGAIN Identity Provider is correctly configured for eduGAIN when it can release all Recommended Attributes to the eduGAIN Service Providers.

A useful service that permits to you to quickly test this for your Identity Provider is the **eduGAIN Attribute Release Check.**

This service consists of several Service Providers with different attribute settings and entity categories. Starting the check a user will log in on these services, which then check which attributes were released by the Identity Provider. At the end, a test verdict will be shown.

If the Identity Provider failed the test, its users **may not** have access to other eduGAIN services because the services MAY require some of the recommended attributes. **May not** is emphasized because it is important to understand that an Identity Provider **does not have to** release the recommended attributes to **all** eduGAIN services **every time**. The eduGAIN Release Check only checks if an Identity Provider is able to release this set and therefore the test is only an indication of which attributes (or a subset thereof) may be requested by the eduGAIN services.

A Home Organisation has some responsibility when it releases attributes about their users to an SP. The user data is sent to a Service Provider, which may store it. If the SP is compromised, the user's personal data may be spilled to the Internet. Also, Service Providers may be operated by commercial companies which sometimes tend to request as many user information as possible.

In the interfederation/eduGAIN context there are two concepts (entity categories) that are relevant for a responsible attribute release: The GÉANT Data Protection Code of Conduct and the "REFEDS Entity Category Research and Scholarship. Both are SAML entity categories, which classify Service Providers that commit to certain rules and/or meet certain requirements. Both concepts, which are orthogonal to each other, allow to create easier and safer attribute release rules. Therefore, it is recommended to support one or both of them.

Additional eduGAIN Services Recommended for Testing

If the Identity Provider successfully passed the above-mentioned Attribute Release Check, the next step could be testing access to some eduGAIN service that are open to use for all users of eduGAIN-enabled Identity Provider. Some of these services are listed below:

Service	Required Attributes	Description
AAI Viewer Interfederation Test	email, eduPersonAffiliation, eduPersonPrincipalName, eduPersonTargetedID, eduPersonScopedAffiliation, displayName, commonName, schacHomeOrganization, schacHomeOrganizationType	This service is used to test the interfederation readiness of SWITCHaai Identity Providers.
eduGAIN Wiki	eduPersonTargetedID, eduPersonPrincipalName	This wiki provides recommendations and instructions on how to enable web services for eduGAIN.
AAI Attribute Viewer	preferredLanguage, email, homePostalAddress, postalAddress, homePhone, telephoneNumber, mobile, eduPersonAffiliation, eduPersonOrgDN, eduPersonOrgUnitDN, eduPersonEntitlement, surname, givenName, uid, employeeNumber, ou, eduPersonPrincipalName, eduPersonAssurance, eduPersonTargetedID, eduPersonPrimaryOrgUnitDN, primaryGroupID, isMemberOf, eduPersonNickname, eduPersonScopedAffiliation, eduPersonPrimaryAffiliation, displayName, commonName, schacHomeOrganization, schacHomeOrganizationType	Displays all available attributes of a user for debugging and informational purposes.
GEANT Intranet	email	A collaboration platform for GÉANT Project participants
~okeanos global	eduPersonTargetedID	~okeanos is a brand new IaaS Service. "IaaS" stands for "Infrastructure as a Service". This means that you can build your own computer, always connected to the Internet, without worrying about hardware failures, spaghetti cables, connectivity hiccups and software troubles.
Shibboleth.net Wiki	cn, displayName, eduPersonPrincipalName, eduPersonTargetedID, mail	The wiki hosting the documentation for Shibboleth. Unauthenticated users may view the existing documentation. Authenticated users may create new documentation pages and edit existing ones.