eduGAIN Connectivity Check

The purpose of the eduGAIN Connectivity Check is to identify eduGAIN Identity Providers (IdP) that are not properly configured. In particular it checks if an IdP properly loads and consumes SAML2 metadata which contains the eduGAIN Service Providers (SP). The check results are published on the public eduGAIN Connectivity Check web page (https://technical.edugain.org/eccs/). The main purpose is to increase the service overall quality and user experience of the eduGAIN interfederation service by making federation and Identity Provider operators aware of configuration problems.

The check is performed by sending a SAML authentication request to each eduGAIN IdP and then follow the various HTTP redirects. The expected result is a login form that allows users to authenticate (typically with username/password) or an error message of some form. For those Identity Providers that output an error message, it can be assumed that they don't consume eduGAIN metadata properly or that they suffer from another configuration problem. There are some cases where the check will generate false positives, therefore IdPs can be excluded from checks as is described below.

The Identity Providers are checked once per day. Therefore, the login requests should not have any significant effect on the log entries/statistics of an Identity Provider. Also, no actual login is performed because the check cannot authenticate users due to missing username and password for the IdPs. Only Identity Providers are checked but not the Service Providers.

If this page does not answer to your questions or you need some more information about this service, please contact us on support@edugain.org.

Check Performed on the IdPs

The check executed by the service follows these steps:

1. It retrieves the eduGAIN IdPs from eduGAIN Operator Team database via a JSON interface
2. For each IdP that is was not manually disabled by the eduGAIN Operations Team, the check creates a SAML Authentication Request message to send to the location of the first "**SingleSignOnService**" URL with binding "**urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect**" in SAML metadata for that IdP.
   The SPs used for the check are "**Test SP shib 2.4**" (https://sp24-test.garr.it/shibboleth) from IDEM GARR AAI and the "**AAI Viewer Interfederation Test**" (https://attribute-viewer.aai.switch.ch/interfederation-test/shibboleth) from SWITCHaai. These SPs might change in the future if needed.
   The SAML authenticatin request is not signed. Therefore, authentication request for any eduGAIN SP could be created because the SP's private key is not needed.
3. The SAML Authentication Request is sent and the IdP login page is retrieved by the check. It expects to find the HTML form with a username and password field. Therefore, no complete login will happen at the Identity Provider because the check stops at the login page.

Limitations

There are some situations where the check cannot work reliably. In those cases it is possible to disable the check for a particular IdP. The so far known cases where the check might generate a false negative are:

- IdP does not support HTTP or HTTPS with at least SSLv3 or TLS1 or newer (these IdPs are insecure anyway)
- IdP is part of a Hub & Spoke federation (some of them manually have to first approve eduGAIN SPs)
- IdP does not use web-based login form (e.g. HTTP Basic Authentication or X.509 login)

Disable Checks

In cases where an IdP cannot be reliably checked, it might be necessary to disable the checks for an IdP.

On-line interface

The eduGAIN Connectivity Check web pages is available at: https://technical.edugain.org/eccs/

The tool uses following status for IdPs:

Status	Color	Decription
Error	**Red**	The IdP's response contains an HTTP Error or the web page returned does not look like a login page. The most probable causes for this error are HTTP errors (e.g.: 404 error).

Warning	**Orange**	The IdP most likely does not consume the eduGAIN metadata correctly or it hasn't does not return a web page that looks like a login form. A typical case that falls into this category is when an IdP returns a message "No return endpoint available for relying party" or "No metadta found for relying party".
OK	**Green**	The IdP most likely correctly consumes eduGAIN metadata and returns a valid login page. This is no guarantee that login on this IdP works for all eduGAIN services but if the check is passed for an IdP, this is probable.
Diasable	**White**	The IdP is excluded from checks because it cannot be checked reliably (see limitations below) affected by some problems that prevent them to consume correctly eduGAIN metadata. The "*Last test results*" column, when an entity is disabled, shows the reason of the disabling

The eduGAIN Connectivity Check's administrator can disable checks for entities by changing the service database. This is useful because some Identity Providers use login methods that cannot easily/reliably be checked. Therefore such IdPs should be excluded from the checks.

JSON interface

The eduGAIN Connectivity Check service provides also a JSON feed on the monitoring results in: https://technical.edugain.org/eccs/services/json_api.php

It is possible to change the page of the results by inserting the number of the page in an URL like this:

```
https://technical.edugain.org/eccs/services/json_api.php?action=###ACTION-NAME###&page=###PAGE-NUMBER###
```

The table below describes the JSON feed and the action that can be performed by replacing ##ACTION## in the URL:

```
https://technical.edugain.org/eccs/services/json_api.php?action=##ACTION##
```

Action name (JSON)	Action description
entities	List all the eduGAIN Connectivity Check service results.
checks	List all the checks on the eduGAIN IdPs performed by eduGAIN Connectivity Check service.
fedstats	List all the federation statistics collected by the eduGAIN Connectivity Check service.

The table below, instead, describes the JSON parameters that an action can use:

Parameter name (JSON)	Parameter description
f_order	• **All**: no order • **displayName**: order by DisplayName • **entityID**: order by entityID • **registrationAuthority** (only for "entities" action): order by registrationAuthority • **ignoreEntity**: order by ignoredEntity • **lastCheck**: order by last check • **currentResult**: order by last result
f_order_direction	• **ASC**: ascending order • **DESC**: descending order
f_entityID	• **All**: consider all entityIDs • **A specific IdP's entityID value**: consider only a specific one
f_registrationAuthority	• **All**: consider all registrationAuthorities • **A specific registrationAuthority value**: consider only a specific one

f_displayName	- **All**: consider all DisplayName - **A specific IdP's DisplayName value**: consider only a specific one
f_ignore_entity	- **True**: for the entities that are ignored (by the service owner). - **False**: for the entities that are considered (by the service owner).
f_current_result (for only "checks" action)	- **All**: consider all IdPs - **OK**: consider only IdP that have received an "OK" from the check script. - **FORM-Invalid**: consider only IdP that have received an "FORM-Invalid" from the check script - **HTTP-Error**: consider only IdP that have received an "HTTP-Error" from the check script - **TCP/IP-Error**: consider only IdP that have received an "TCP/IP-Error" from the check script
rpp	- **All**: Show all entities - **20**: Show 20 entities per page. (default value: 30)

Example URL:

```
https://technical.edugain.org/eccs/services/json_api.php?action=entities&f_registrationAuthority=https%3A%2F%2Fwww.aai.dfn.de&rpp=All
```