Configuring an SP for eduGAIN

After meeting the organisational requirements for joining eduGAIN, the SP needs to meet the following technical requirements:

- Run up-to-date software
- Declare R&S (recommended if applicable)
- Declare SIRTFI and provide SIRTFI contact (recommended)
- Provide a logo representing the service
- Provide a page with further information about the service (InformationURL)
- Load eduGAIN metadata
- Request attributes needed
- Use eduGAIN-enabled Discovery Service

The final step is to send the Request to Join eduGAIN to Tuakiri/REANNZ.

This page provides further details on these technical requirements. For the details of the full process of joining eduGAIN, please see the eduGAIN Information Pack.

Running up-to-date SP software

The SP MUST run a supported SAML implementation with all security updates applied (e.g., latest Shibboleth SP).

Declaring R&S

Please see the eduGAIN Information Pack and the REFEDS Research and Scholarship Category definition for full details.

In essence:

- R&S Service Providers are SPs that support Research and Scholarship activities and request only a small selection of attributes (see the above link for details)
- IdPs declare support for R&S by agreeing to release these attributes.

If an SP declares it meets the SP R&S requirements (the purpose of the SP is to support Research and Scholarship activities), the SP can expect that IdPs supporting R&S will release the attributes defined in the R&S attribute bundle.

The actual declaration of support for R&S will be part of the joining request sent to Tuakiri as per the instructions in the eduGAIN Information Pack.

SIRTFI

SIRTFI (Security Incident Response Trust Framework for Federated Identity) is a lightweight framework to request and provide security incident response assistance, publish security incident contact information and review security incident capability.

For SPs, SIRTFI is highly recommended for joining eduGAIN. Organisations self-assess against the SIRTFI criteria and then self-assert SIRTFI. They also have to provide a security contact - which should be a role-based email address, not personal.

- The security contact should be provided by adding the contact as a `security` contact of the IdP in the Tuakiri Federation Registry.
- The step of self-asserting SIRTFI is included in the request to join eduGAIN as per the instructions in the eduGAIN Information Pack.

For more information, please see the eduGAIN Information Pack and the REFEDS SIRTFI documentation.

Logo

An SP should provide a logo to help users with confirm they are logging into the right service when the logo is displayed on the IdP login page (and possibly also the Discovery Service).

To provide a logo, please include an **HTTPS** link to your logo in your request to join eduGAIN. The Tuakiri team will take care of including the logo in the metadata sent to eduGAIN.

Information URL

The registration data for an IdP or SP in the Federation Registry include a (human readable) name and a description - which get included in the generate metadata.

For a Service Provider, it is highly recommended to provide a URL to page with further information about the service, which will be published into the eduGAIN metadata as `InformationURL`.

Loading eduGAIN metadata

Tuakiri provides a version of the eduGAIN metadata tailored for consumption by Tuakiri members.

The eduGAIN metadata is signed with the same certificate as the Tuakiri metadata - and is published separately for the Production and TEST federations.

Note that there is no TEST eduGAIN federation, so test SPs cannot do full end-to-end eduGAIN testing, but partial tests can still confirm the configuration has been applied to the SP correctly, and that's what the eduGAIN metadata stream for TEST is for.

The metadata URL and signing certificate are:

Federation name	Tuakiri	Tuakiri TEST
Metadata name	**tuakiri.ac.nz/edugain-verified**	**test.tuakiri.ac.nz/edugain-verified**
Metadata distribution point	https://directory.tuakiri.ac.nz/metadata/tuakiri-edugain-verified.xml	https://directory.test.tuakiri.ac.nz/metadata/tuakiri-test-edugain-verified.xml
Metadata signing certificate	https://directory.tuakiri.ac.nz/metadata/tuakiri-metadata-cert.pem	https://directory.test.tuakiri.ac.nz/metadata/tuakiri-test-metadata-cert.pem

To load the metadata, add the following snippet in `/etc/shibboleth/shibboleth2.xml` just **BELOW** the snippet loading the Tuakiri metadata

Tuakiri (PRODUCTION): load eduGAIN metadata

```
<MetadataProvider type="XML" url="https://directory.tuakiri.ac.nz/metadata/tuakiri-edugain-verified.xml"
        backingFilePath="metadata.tuakiri-edugain.xml" reloadInterval="7200" validate="true">
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="2419200"/>
    <MetadataFilter type="Signature" certificate="tuakiri-metadata-cert.pem" verifyBackup="false"/>
    <MetadataFilter type="EntityRoleWhiteList">
        <RetainedRole xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">md:IDPSSODescriptor</RetainedRole>
    </MetadataFilter>
</MetadataProvider>
```

Tuakiri-TEST: load eduGAIN metadata

```
<MetadataProvider type="XML" url="https://directory.test.tuakiri.ac.nz/metadata/tuakiri-test-edugain-
verified.xml"
        backingFilePath="metadata.tuakiri-test-edugain.xml" reloadInterval="7200" validate="true">
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="2419200"/>
    <MetadataFilter type="Signature" certificate="tuakiri-test-metadata-cert.pem" verifyBackup="false"/>
    <MetadataFilter type="EntityRoleWhiteList">
        <RetainedRole xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">md:IDPSSODescriptor</RetainedRole>
    </MetadataFilter>
</MetadataProvider>
```

Requesting Attributes

Your SP should have the list of requested attributes recorded in the Federation Registry as part of the initial registration. If not sure, please check that the attributes your SP needs match what is recorded in the Federation Registry.

The same list of requested attributes will be used for Tuakiri and for eduGAIN - the list of requested attributes will be included in the SP metadata published into eduGAIN. But please be aware that not all IdPs in eduGAIN will be supporting (and releasing) the same set of attributes in Tuakiri.

Attributes in the R&S Attribute bundle should be released by all IdPs supporting R&S. Other attributes may be released depending on the IdP configuration.

Configuring Discovery Service to use

Service Providers rely on a Discovery Service to let their users select the IdP to use. When connecting an SP to eduGAIN, the Discovery Service has to offer the full list of all IdPs in eduGAIN. Tuakiri provides a centralised Discovery Service that can be used by Tuakiri-only SPs as well as eduGAIN-enabled SPs.

If your SP is using the Tuakiri Discovery Service, to become eduGAIN enabled, the SP must start using a different endpoint on the Discovery Service, configured to render also a separate tab for eduGAIN IdPs (labelled "International"). In `/etc/shibboleth/shibboleth2.xml` , change the `discovery URL` in the `SSO` element to `https://directory.tuakiri.ac.nz/discovery/edugain` (or `https://directory.test.tuakiri.ac.nz /discovery/edugain` for Tuakiri-TEST):

```
<SSO
     discoveryProtocol="SAMLDS" discoveryURL="https://directory.tuakiri.ac.nz/discovery/edugain">
  SAML2
</SSO>
```

Applying Changes - Restart

Changes to `/etc/shibboleth/shibboleth2.xml` are picked up automatically and no restarts are needed. If for some reason the changes do not get picked up, the service to restart are the Shibboleth daemon (`shibd`) and Apache (`httpd` on RedHat and `apache2` on Debian/Ubuntu).

Please note that due to the size of the eduGAIN metadata, ShibSP may take a few minutes to restart if refreshing the metadata at the time of startup (the delay is on the signature checking of the downloaded eduGAIN metadata). In normal operation, the refresh happens in the background, without impacting service performance.