

Information pack

International connectivity for Australian Access Federation (AAF) Subscribers who want to connect their Service Providers (SP) to eduGAIN.

What is eduGAIN?

eduGAIN (Education Global Authentication Infrastructure) enables researchers, educators and students in one country to collaborate with their colleagues and access applications, tools and datasets in other countries.

eduGAIN is a global initiative to connect federations around the world. For more information, go to www.geant.org/Services/Trust_identity_and_security/eduGAIN

The AAF is now connected to eduGAIN and Service Providers can open their services to international researchers if desired. This information pack outlines the steps Service Providers must take to connect to eduGAIN.

Why should I connect my service to eduGAIN?

By connecting to eduGAIN, your service will benefit from:

- ▶ exposure to international end-users who can access your service(s) via other international federations
- ▶ simplified and secure information exchange for access and authentication
- ▶ international research collaboration
- ▶ simple and secure access for researchers, removing the need for direct integration with applications in other federations.

What does my organisation need to do to connect to eduGAIN?

Requirements to connect to eduGAIN

Connecting to eduGAIN is optional however there are requirements that must be met before connecting.

	SAML Software implementation	Technical Connection requirements	R&S Research & Scholarship Entity Category	SIRTFI Security Incident Response Trust Framework for Federated Identity
SP	Run the latest version of software	Consume Metadata, discovery mechanism and request attributes	Recommended for qualifying services	Recommended

How to connect

- Step 1:** Complete the Connect to eduGAIN form to indicate your organisation's intent to connect to eduGAIN.
- The Primary Representative for your organisation's AAF Subscription must complete this form.
- Step 2:** Complete the necessary requirements to connect to eduGAIN.
- Refer to Requirements to connect to eduGAIN.
- Step 3:** Notify AAF Support that you have completed the requirements.
- Email: support@aaf.edu.au
 - Complete the template (refer to Request to join eduGAIN).

Things to consider when connecting to eduGAIN

The AAF recommends reviewing relevant legislation before connecting to eduGAIN.

Australian Privacy Principles (APPs)

The Privacy Act 1988 includes 13 Australian Privacy Principles (APPs) defined at:
www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles

The APPs set out standards, rights and obligations for handling, holding, using, accessing and correcting personal information (including sensitive information).

Service Providers can only use personal information for the purpose of delivering their service and may only disclose this information to other parties in specific situations.

Key privacy principles subscribers should consider:

For Service Providers

- APP 2 — Anonymity and pseudonymity
- APP 4 — Dealing with unsolicited personal information
- APP 6 — Use or disclosure of personal information

AAF Subscribers should review their obligations as they prepare to connect to eduGAIN. AAF Subscribers should consider other privacy principles that may apply to them.

State and Territory Privacy Legislation

Service Providers may be subject to other state-based requirements. The AAF recommends reviewing relevant legislation for applicability before connecting to eduGAIN.

Australian Capital Territory

Information Privacy Act 2014 (ACT)

New South Wales

Privacy and Personal Information Protection Act 1998 (NSW)

Health Records and Information Privacy Act 2002 (NSW)

Northern Territory

Information Act (NT)

Queensland

Information Privacy Act 2009 (Qld)

South Australia

Privacy Committee of South Australia

Tasmania

Personal Information and Protection Act 2004 (Tas)

Victoria

Privacy and Data Protection Act 2014 (Vic)

Western Australia

Freedom of Information Act 1992 (WA)

SAML software implementation

What does my organisation need to do with its SAML software implementation?

All AAF Subscribers are required to observe good practice in relation to the configuration, operation and security of their connections to the Federation. In order to achieve this you will need to make sure that the Service Provider software connecting to eduGAIN is running the latest version.

Technical connection requirements

There are a number of technical requirements your organisation's SPs must follow to connect to eduGAIN. Requirements cover metadata consumption, attribute consumption and discovery for SPs. Specific information about the technical requirements to connect to eduGAIN are available via the AAF Knowledge Base (support.aaf.edu.au) or by contacting support@AAF.edu.au

eduGAIN metadata

The AAF supplies a new metadata source for eduGAIN that provides the technical trust for the international connection. Whether you run an IdP or an SP, you must consume this new metadata to connect to eduGAIN. This will require some minor configuration changes to your SP.

Attribute consumption (for SPs)

Service Providers must ensure their attribute requirements are recorded in the AAF Federation Registry. These requirements will be made available to IdPs in eduGAIN via metadata.

Discovery mechanism (for SPs)

The AAF and international federations rely on the Discovery Service (also referred to as the 'Where Are You From' service) to help end-users identify which IdP to login to. The AAF Discovery Service has been extended to include all eduGAIN IdPs. A simple change to the discovery URL in your Shibboleth SP configuration will enable the eduGAIN IdPs.

Your service can provide its own discovery mechanism rather than using the AAF's Discovery Service. The eduGAIN metadata that your service consumes will include all of the Metadata Extensions for Login and Discovery User Interface (MDUI) information that your service's discovery mechanism will require.

Research and Scholarship (R&S) Entity Category

What is R&S?

The Research and Scholarship (R&S) Entity Category establishes a baseline attribute set that all research-related IdPs and SPs agree to exchange. The R&S Entity Category is an initiative of the international Research and Education Federations (REFEDS) community.

Why does my service need to assert R&S?

If your service qualifies for R&S (refeds.org/category/research-and-scholarship), we recommend that SPs request the AAF to assert R&S on the SP's behalf. Service Providers asserting R&S can trust they will receive the attributes they need to authorise access. If an SP does not qualify for R&S they will need to develop an SP integration guide to distribute to international IdPs that want to use the service.

How do I assert R&S?

Asserting R&S

For Service Providers

Asserting R&S means:

"I meet the requirements of the R&S category. I expect to receive attributes defined in the R&S specification from IdPs indicating they support R&S"

If an SP meets the R&S Registration Criteria (refeds.org/category/research-and-scholarship) then you can expect to receive these attributes from an IdP asserting R&S.

R&S Attribute Bundle

The R&S attribute bundle consists of the following required data elements:

- shared user identifier
- person name
- email address

and one optional data element:

- affiliation

The shared user identifier is a persistent, non-reassigned, non-targeted identifier defined to be either of the following:

1. eduPersonPrincipalName (if non-reassigned)
2. eduPersonPrincipalName + eduPersonTargetedID

Person name is defined as either (or both) of the following:

1. displayName
2. givenName + sn

Email address is defined as the mail attribute. Affiliation is defined as the eduPersonScopedAffiliation attribute.

For more information about the R&S Entity Category, go to refeds.org/category/research-and-scholarship

SIRTFI

Security Incident Response Trust Framework for Federated Identity (SIRTFI).

What is SIRTFI?

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

Why does my organisation need to use SIRTFI?

SIRTFI is an important global framework covering good practice for communicating about security incidents in an effective and timely manner. SIRTFI helps security contacts know who to contact in other organisations and the best channels to use. The SIRTFI framework is an initiative of REFEDS.

How does my organisation assert SIRTFI?

Assert SIRTFI

Step 1: Read and understand the SIRTFI framework requirements.

- Go to refeds.org/sirtfi
- View the SIRTFI Framework (refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf)

Step 2: Self-assess your organisational capability against the SIRTFI requirements.

Step 3: Provide your security contact information to the AAF to share with security contacts in other federations.

- Update your contact details in Federation Registry or contact AAF Support support@aaf.edu.au
- Notify AAF Support that you have met the SIRTFI requirements.

Step 4: Notify AAF Support when contact details change.

SIRTFI Framework

The SIRTFI framework (refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf) requires organisations to self-assess against the following areas:

OPERATIONAL SECURITY (OS)	INCIDENT RESPONSE (IR)	TRACEABILITY (TR)	PARTICIPANT RESPONSIBILITIES (PR)
Security patches	IR assistance	Retaining records	Acceptable Use Policy (AUP)
Vulnerability management	SIRTFI IR assistance	Audit trails	User acknowledgement of AUP
Threat detection	Collaboration		
User access rights	IR procedures		
Contact information	User privacy		
Security incident response	Traffic Light Protocol		

Traffic Light Protocol

Organisations within the SIRTFI community agree to provide a coordinated response to security incidents, including assisting other organisations as required. SIRTFI requires organisations to understand and use the Traffic Light Protocol (TLP) for security incident communications. For more information about TLP, go to www.us-cert.gov/tlp

Request to join eduGAIN

Join eduGAIN email template

For Service Providers (SP)

When your SP is ready to be connected to eduGAIN, email support@aaf.edu.au using the following template.

Dear AAF Support,

We request that the service “____SERVICE NAME____” operated by “____ORGANISATION NAME____” be added to eduGAIN.

We have completed and tested the following technical configuration changes:

- Loading the AAF eduGAIN metadata
- An eduGAIN enabled Discovery Service

We (do / do not) require this service to assert compliance with SIRTFI.

We (do / do not) require this service to assert Research and Scholarly to enable access to R&S attributes.

Additional Security Contacts for your service:

“____NAME____”
“____EMAIL____”
“____PHONE____”