# Application to join eduroam AU:Identity plus Service Provider (IdP+SP) Participant

Prior to completing this form, AARNet will have provided basic information on requirements for eduroam AU participation (a standard information pack via email), and will have accepted your institution as eligible for IdP+SP participation.

The next step in joining eduroam AU is submission of this form via email to: support@aarnet.edu.au.
An AARNet Service Desk ticket will be created and will be used for information exchange during the on-boarding process. Please exchange information with AARNet via the ticket rather than direct email to AARNet staff.

The information provided via this form will be used to ascertain the candidate institution’s ability to comply with [eduroam AU National Policy](https://wiki.aarnet.edu.au/download/attachments/7045184/eduroam-national-policy_v4.2.pdf?version=1&modificationDate=1496190358356&api=v2), and its technical readiness to operate in eduroam AU as an IdP+SP participant.

Following review and any required clarification, AARNet will invite the institution to commence deployment as an IdP+SP participant, and will register the institution and pre-populate some data, and create an administrator account in the [eduroam AU AdminTool](https://admin.eduroam.edu.au) and invite the administrator to activate their account and commence updating the entry. During the deployment stage, prior to the final audit stage, the deployment status of the institution must be marked as “Staging”.

The information requested in this form is quite comprehensive and reflects the data that is required to be added for the institution to the eduroam AdminTool. If there are any items which you cannot decide on or do not understand, please mark as “TBC” (to be confirmed) or if not applicable (e.g. due to a previous item response), mark as “NA” (not applicable). Information provided will be used to pre-populate the institution’s entry in the eduroam AU AdminTool prior to inviting the designated institutional eduroam administrators (see contacts below) to access, check and take responsibility of data entry going forward.

## Compliance Requirement

### Identity Provider

Identity provider institutions are responsible for their users. Users must adhere to the network Acceptable Use Policy of their home institution. AARNet, as the eduroam AU National Roaming Operator (NRO), is responsible for institutional compliance with the eduroam Global Policy (the [eduroam Compliance Statement](http://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf)). This is accomplished by creation of an [eduroam AU National Policy](https://wiki.aarnet.edu.au/download/attachments/7045184/eduroam-national-policy_v4.2.pdf?version=1&modificationDate=1496190358356&api=v2) that institutions must comply with. Operation as an Identity Provider in eduroam AU is available only to AARNet customers unless AARNet accepts an institution’s IdP participation as an exception based on its business relationship.

### Service Provider

Service provider institutions must comply with the eduroam AU National Policy, which refers to the eduroam Technical Specification. Operation as a Service Provider in eduroam AU is available to any institution with institutional capabilities enabling eduroam policy compliance, and a business case supporting the effort required for compliance.

## General Information

### Institution

|  |  |  |
| --- | --- | --- |
| Institution Name |  Formal name of institution |  |
| Institution Primary DN |  Primary domain name of institution |  |
| Homepage |  Institution website public URL |  |
| Acceptable Use Policy |  Institution network AUP public URL |  |
| Privacy Policy |  Privacy Policy URL |  |

The institution primary domain name will be used as the institutional identifier for metrics and monitoring purposes.

eduroam Deployment Responsibility:

|  |  |  |
| --- | --- | --- |
| 3rd Party Deployment |  (Yes/No) |  |
| Policy requirements clear |  with 3rd Party deployer (Yes/No) |  |

### Institutional Contact(s)

Provision of institutional contacts is required in order to ensure information flow between AARNet and institutions (e.g. institutional operability support, security advisories) and between participating institutions (e.g. user support and troubleshooting, reports for action related to AUP non-compliance). It is preferred that the primary technical contact is a personal contact rather than group.

Institutional technical contacts marked as ‘public’ (at least one ‘Primary Technical’ ‘public’ contact is required) will be shared globally (via a data feed from the eduroam AU AdminTool to the eduroam Global Database).

Institutional technical contacts will be subscribed to the eduroam AU Administrator mailing list.

Institutions are requested to keep eduroam administrative contact information up-to-date, with changes reflected within one business day, via the eduroam AU AdminTool.

#### For each institutional contact:

(Copy and paste table for each contact)

|  |  |  |
| --- | --- | --- |
| Description | e.g. Primary, Secondary Technical |  |
| Name | First Last |  |
| Phone | Mobile is preferable |  |
| Email | Institutional email |  |
| Public (No=private) | Public = shared globally (Yes/No) |  |
| Personal (No=Group) | Personal = individual (Yes/No) |  |
| Designated eduroam admin | Must be “Personal” (Yes/No) |  |
| Administers AdminTool | Must be a designated eduroam admin (Yes/No) |  |

Designated eduroam Administrators will be the addressees (To:) on any correspondence regarding eduroam from AARNet to the institution, and will be the contact provided to other institutions by AARNet if institution-institution contact is required. Other contacts will be copied (Cc:) on correspondence. Public contacts will be shared via the eduroam AU AdminTool data feed (XML file) to the eduroam Global Database.

### Institutional RADIUS Server(s)

The eduroam AU Technical Specification details technical requirements for joining eduroam AU, including the requirements for Institutional RADIUS Servers (IRSs) operated by eduroam IdPs and SPs. The items in this section reflect the general (both IdP & SP) requirements. Role specific RADIUS Server requirements are reflected in subsequent IdP and SP sections.

|  |  |  |
| --- | --- | --- |
| Number of RADIUS Servers | Dual redundancy recommended |  |

#### For each RADIUS Server:

(Copy and paste table for each RADIUS server)

|  |  |  |
| --- | --- | --- |
| RADIUS implementation | Vendor and version |  |
| IP address | Public IPv4 address |  |
| Domain Name | Public domain name |  |
| Auth/Acct Ports | UDP 1812 / 1813 recommended |  |
| RADIUS Attributes compliance | As per Technical Spec. (Yes/No) |  |
| Test & Monitoring Server trust | Configure trust for TMS (Yes/No) |  |
| Status Server capability | (Yes/No) |  |
| Server time synced accurately  | E.g. NTP (Yes/No) |  |
| RADIUS transaction logging | As per Technical Spec. (Yes/No) |  |
| Log timestamps UTC | (Yes/No) |  |
| Log retention period | 3 months minimum |  |

A RADIUS secret (the preferred format being 16 random alphanumeric characters) used to establish trust between institutional RADIUS servers (IRSs) and the National RADIUS Servers (NRSs) and will be generated by AARNet and informed to the institution during deployment.

### eduroam AU AdminTool

Institutions are responsible for maintaining up-to-date deployment data in the eduroam AU AdminTool.

|  |  |  |
| --- | --- | --- |
| Agreement to keep up-to-date  | Update within 1 bus. day (Yes/No)  |  |
| Institutional SAML IdP | (Yes/No) |  |
| Subscriber to the [AAF](https://aaf.edu.au/) | (Yes/No) |  |
| Existing AAF VHO Account  | (Yes/No) |  |
| Global Sharing Consent | Data fed to Global Db (Yes/No)  |  |

AARNet will add the institution to the [eduroam AU AdminTool](https://admin.eduroam.edu.au/), pre-populate some data, and create the institutional administrator accounts and invite administrators to activate their accounts via email.

Access to the eduroam AU AdminTool (and the eduroam Configuration Assistant Tool for IdPs) is via SAML authentication. Many Australian R&E institutions operate a SAML Identity Provider and subscribe to the [Australian Access Federation](https://aaf.edu.au/) (AAF), which enables them to login to the eduroam AU AdminTool. AARNet hosts a SAML proxy that can be used to support SAML login for users from institutions that are not AAF subscribers.

If both SAML IdP and existing VHO Account are “No”, AARNet will create individual SAML accounts for institutional administrators under the AARNet group in the [AAF Virtual Home Organisation](https://vho.aaf.edu.au/).

### Institutional eduroam AU Participation Webpage

|  |  |  |
| --- | --- | --- |
| eduroam webpage URL | Must be a public page |  |
| Compliance with template | Commit to comply (Yes/No) |  |

A public eduroam participation webpage must be created containing information complying with the template provided as part of the ‘joining eduroam AU standard information package’.

The intent of the institutional eduroam participation webpage is to enable local users and visitors to understand the eduroam service and avoid unnecessary calls to eduroam support.

### Institutional Support Capability

|  |  |  |
| --- | --- | --- |
| eduroam Support Capability | Institutional IT Support (Yes/No) |  |
| email address | Institutional email address |  |
| phone number | Phone contact |  |
| Training of support resources | Training to be undertaken (Yes/No) |  |
| Service Request (SR) tracking  | Vendor/software/database |  |
| SR escalation understood | Institution vs AARNet role (Yes/No) |  |

Institutions are required to provide support for eduroam users, both local users remotely authenticated when accessing a visited institution “eduroam” network, and visitors who are accessing the institution’s “eduroam” network.

For eduroam support issues that Institutions are unable to resolve, a support request should be submitted to AARNet via mailto: support@aarnet.edu.au

Basic eduroam support training resources are available from AARNet.

## Identity Provider Specific Information:Users, Realms, Identity Management, Authentication

### Users

|  |  |  |
| --- | --- | --- |
| User Cybersecurity Awareness | E.g. User training (Yes/No) |  |
| AUP compliance required | AUP agreement in place (Yes/No) |  |
| Password security mechanism | e.g. Timed password reset |  |
| Number of eduroam users | Estimated no. of eduroam users |  |

### Authentication

#### For each realm supported:

(Copy and paste tables for each set of institutional realms with different authentication characteristics)

#### Realm identifier:

(Copy and paste the “Realm” row for each realm sharing the same authentication characteristics i.e. identity management, RADIUS configuration, user device configuration, test accounts.)

Institutional realms should have a country-code suffix (i.e. \*.au for eduroam AU).

|  |  |  |
| --- | --- | --- |
| Realm | (Sub)domain-name string |  |

A non-country coded realm should have been discussed with AARNet prior to being invited to submit this application, hence any special reasons for not having an “.au” suffix should have been discussed and agreed.

#### Identity Management:

|  |  |  |
| --- | --- | --- |
| Identity Management System | Vendor & version |  |
| Identity Store | What is the identity store |  |
| Ex-User De-provisioning | Prompt de-provisioning (Yes/No) |  |
| Authentication System logging | Auth logs captured (Yes/No) |  |
| Number of identities | Approximate number of identities |  |

#### RADIUS Authentication:

|  |  |  |
| --- | --- | --- |
| Outer EAP method | EAP-PEAP, EAP-TTLS |  |
| Inner authentication method | MSCHAPv2, PAP |  |
| Send Chargeable-User-Identity | In Access-Accept (Yes/No) |  |
| Accounting Request handling | Accounting response (Yes/No) |  |

#### User device configuration:

|  |  |  |
| --- | --- | --- |
| eduroam configuration @home | Config on home campus? (Yes/No) |  |
| Configuration Assistant Tool | Will CAT scripts be used (Yes/No) |  |
| Other auth config automation | If not CAT, what automation? |  |
| RADIUS Server Cert CN | CN of home RADIUS server |  |
| Signing Root CA Subject | Subject of Root CA |  |

#### Test Account:

|  |  |  |
| --- | --- | --- |
| Institutional test account | eduroam-test@realm |  |
| Provided password  | SMS to 0425 263 946 (Yes/No) |  |

### RADIUS Server IdP Role

#### For each RADIUS server configured for IdP operability:

(Copy and paste tables for each RADIUS Server)

|  |  |  |
| --- | --- | --- |
| IP Address | Must be included in general sect. |  |
| Realms handled | Set/subset of realms above |  |
| Priority | Priority (primary=1, fail-over=2-n) |  |

## Service Provider Specific Information:RADIUS, Wireless, eduroam Network & Coverage

This form assumes your wireless infrastructure is homogenous across your locations regarding eduroam deployment. Please indicate if not and arrange for further information exchange with AARNet.

### Locations

For each distinct institutional location/campus/site where eduroam is provided:

(Copy and paste table for each location).

(Copy and paste the “Location” rows below for each location sharing the same wireless infrastructure, RADIUS server and network service characteristics.)

|  |  |  |
| --- | --- | --- |
| Name | Location name |  |
| Address | Full street address |  |
| Coordinates | Latitude & longitude |  |
| Name of contact | Must be in contacts above |   |

(For locations with different wireless, RADIUS and network service, list separately and copy & paste the appropriate rows reflecting the difference from below).

### Wireless Infrastructure

For eduroam Network Authentication Servers (NAS’s) (Wireless Access Points):

|  |  |  |
| --- | --- | --- |
| Confirm “eduroam” SSID | (Yes/No) |  |
| Confirm WPA2/AES encryption | (Yes/No) |  |
| MAC in Calling-Station-ID | MAC in CSI (Yes/No) |  |
| NAS-IP-Address  | Populated (Yes/No) |   |

eduroam Coverage Map:

|  |  |  |
| --- | --- | --- |
| Wireless coverage map | Public URL (NA if not available) |  |
| Is eduroam coverage same | (Yes/No) |  |
| eduroam coverage map | Public URL (NA if not provided) |  |

### RADIUS Server

The eduroam AU Technical Specification details minimum requirements for joining the eduroam service. These are detailed in the following questions.

|  |  |  |
| --- | --- | --- |
| Send MAC in Calling-Station-Id | Populated (Yes/No) |  |
| Send Framed-MTU value | Avoiding exceeding network MTU |  |
| RADIUS “Operator-Name” | Populated (Yes/No) |  |
| RADIUS “Chargeable-User-Identity” | Requested (Yes/No) |  |
| Invalid User-Name Rejection | Invalid username/realm (Yes/No) |  |
| Realm black-listing | As per Tech Spec (Yes/No) |  |
| Accounting requests proxied? | Should NOT be (Yes/No) |   |
| RADIUS logging compliant | (Yes/No) |   |
| DHCP logging compliant | (Yes/No) |   |
| Retention period for RADIUS logs | 3 months min |   |

###

### eduroam Network Service

#### General:

|  |  |  |
| --- | --- | --- |
| Device network config via DHCP? | (Yes/No) |  |
| Network Address Translation used? | (Yes/No) |  |
| IPv6 address assignment? | (Yes/No) |  |

#### Logging:

|  |  |  |
| --- | --- | --- |
| Network infrastructure logging |  DHCP logs captured (Yes/No) |  |
| Retention period for DHCP logs |  3 months min |   |

#### Proxies:

|  |  |  |
| --- | --- | --- |
| Do outbound HTTP/HTTPS connections require the use of a proxy? | If 'Yes' answer next below. (Yes/No) |  |
| Is the proxy implemented as a transparent proxy? | If ‘Yes’ answer next 2 below (Yes/No) |  |
| Is the proxy discovered via DHCP/DNS entry? |  (Yes/No) |  |
| Is the proxy discovered via a PAC or WPAD entry? |  (Yes/No) |  |

#### Capacity Restrictions:

|  |  |  |
| --- | --- | --- |
| Inbound rate limiting  | Is inbound rate limiting applied (Yes/No) |  |
| Rate limited bandwidth | What is the rate limited shared bandwidth |  |

#### Ports/Protocols enabled (outbound):

Web Server:

|  |  |  |
| --- | --- | --- |
| HTTP & HTTPS | TCP Ports 80 & 443 (Yes/No) |  |

SSH:

|  |  |  |
| --- | --- | --- |
| SSH | TCP Port 22 (Yes/No) |  |

Email:

|  |  |  |
| --- | --- | --- |
| IMAP (2+4, 3, S) | TCP Ports 143, 220, 993 (Yes/No) |  |
| POP (3S) | TCP Ports 110, 995 (Yes/No) |  |
| SMTP (S,STARTTLS) | TCP Ports 465, 587 (Yes/No) |  |

VPN:

|  |  |  |
| --- | --- | --- |
| Standard IPSec VPN | IP Protocols 50 (ESP), 51 (AH) and UDP Port 500 (IKE) (Yes/No) |  |
| PPTP VPN | IP Protocol 47 (GRE) TCP Port 1723 and (Yes/No) |  |
| Cisco IPSec VPN over TCP | TCP Port 10000 (Yes/No) |  |
| OpenVPN v2.0 | UDP Port 1194 (Yes/No) |  |

Miscellaneous:

|  |  |  |
| --- | --- | --- |
| IPv6 Tunnel Broker Service | IP Protocol 41 (Yes/No) |  |
| IPSec NAT Traversal | UDP Port 4500 (Yes/No) |  |
| Passive (S)FTP | TCP Port 21 (Yes/No) |  |
| RDP | TCP Port 3389 (Yes/No) |  |

In many eduroam jurisdictions (e.g. UK, US) the protocols above are the required minimum services that are available to all users connecting to the SP’s “eduroam” network.

For eduroam AU, these are strongly recommended, and if not provided the rationale should be discussed with AARNet.

The network service provided must be described on the institution’s eduroam webpage, hence any departure from the above will be informed to users via that webpage.

## Appendix A: Workflow following submission of the Application

You may receive notification via the created support ticket during review of your application seeking any required clarification. Once all clear, you will receive further notification inviting you to proceed with RADIUS server deployment and/or configuration, eduroam AU participation webpage creation, support capability preparation, access to the eduroam AU AdminTool & the eduroam CAT.

SP participants will receive notification of the AARNet eduroam AU Test & Monitoring Server (TMS) Account, which will be of the form your\_realm@test.eduroam.edu.au.

During institutional and national RADIUS server configuration, IdP participants’ institutional test accounts will be used to test eduroam IdP operability, and the eduroam AU TMS account will be used to test SP participant’s eduroam SP operability.

An institution’s operational status during deployment activities will be denoted as “Staging” in the eduroam AU AdminTool. No data for the institution will be sent to the Global Database, and the institution will not appear as a participant in the eduroam AU AdminTool public interface or eduroam AU website.

At the appropriate time, following deployment, a final audit will be conducted. At that time the institution’s operational status will be denoted as “Pre-Production”, and following confirmation of XML data for the institution, data from the eduroam AU AdminTool will be made available to the Global Database, hence to the Configuration Assistant Tool CAT. The Final Audit will involve IdP institutions using the scripts generated by the CAT for end-user device configuration.

Following successful Final Audit, the institutional operational status will be denoted as “Production”.

## Appendix B: eduroam AU Infrastructure Information

The following servers are hosted by AARNet, and will be required to be configured in RADIUS servers, with primary/fail-over order dependent on you location (NRS locations inferred from domain names). Please configure using the anycast address of the NRSs.

### National RADIUS Servers

Domain name:
IP Address: 202.158.207.10 (Use this anycast address in RADIUS configuration)
Port: Auth 1812 / Acct 1813
Secret: To be conveyed offline
Status Server: Yes

Domain name:
IP Address: 202.158.207.11 (Use this anycast address in RADIUS configuration)
Port: Auth 1812 / Acct 1813
Secret: To be conveyed offline
Status Server: Yes

### Test & Monitoring Server

Institution are required to configure trust in each of their RADIUS servers for the eduroam AU Test & Monitoring Server, which operates as a RADIUS client.

The RADIUS software client “rad\_eap\_test” is used to issue requests directly from the TMS to institutional RADIUS Servers.

Domain name: TBA
IP Address: TBA
Port: Auth 1812 / Acct 1813
Secret: Use same as between IRS & NRS
Status Server: Yes

eduroam AU Test & Monitoring accounts are created for SP institutions in the eduroam AU Test & Monitoring RADIUS Server, which run FreeRADIUS.