eduroam AU Process

aarnet
Australia's Academic and Research Network

eduroam

Contents

NOTATION

Notation adopted in this document is as defined in IETF RFC 2119.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1. BACKGROUND TO THIS DOCUMENT

This process document for eduroam AU must be read in conjunction with the eduroam AU policy.

1.1 What is eduroam?

1.1.1. **eduroam (education roaming)** is the secure, global roaming access service. It allows any user from participating institution to get network access at any other institutions connected to eduroam.

1.1.2. eduroam **SP (Service Provider)** is the institution that facilitates user authentication and provides network access to successfully authenticated eduroam users.

1.1.3. eduroam **IdP (Identity Provider)** is the eduroam user's home institution that provides user credential and performs user authentication.

1.1.4. **User** from an eduroam identity provider (IdP) institution automatically access the network of a visited eduroam service provider (SP) institution by virtue of the user's successful remote authentication by their IdP (home institution).

1.1.5. eduroam may be used for wired or wireless network access. For wireless access, a standard SSID "eduroam" is broadcast at each eduroam SP.

1.1.6. Standardised network naming and user-device pre-configuration including credential storage enables automatic authenticated network access by eduroam users when they visit eduroam locations.

1.1.7. This document describes requirements and recommendations pertaining to an eduroam AU institutional participant's roles and responsibilities. It is intended to both satisfy the Global eduroam Policy, the AARNet Pty Ltd (AARNet) eduroam policy requirements and to describe eduroam AU specific requirements and recommendations to facilitate achievement of AARNet's operational objectives for eduroam AU.

1.1.8. Appendices A and B of this document describe administrative and technical requirements for institutional participation in eduroam AU.

1.1.9 An eduroam AU institutional participant (hereafter referred to as "**the Institution**" or "**Participant**") MUST comply with this document.

2. AUTHORITY AND COMPLIANCE

2.1.1. The Institution's participation of eduroam AU is interpreted as acceptance of this document by the Institution.

2.1.2. If AARNet identifies non-compliance with this document, AARNet will notify the Institution's designated eduroam administrator by email of the breach and describe the required resolution. Where such notifications are not acted upon in a timely manner, AARNet reserves the right to block the Institution's participation in eduroam.

2.1.3 In case of non-compliance where immediate action is deemed necessary by AARNet to protect the integrity and security of eduroam, AARNet reserves the right to block the Institution's participation immediately without prior notice and advise the Institution's eduroam administrator of the action, breach and required resolution.

2.1.4 In case of any event or behaviour constituting a threat to the security of eduroam, where immediate action is deemed necessary by AARNet to protect the security of Participants, AARNet reserves the right to suspend

eduroam AU immediately and take appropriate action.

3. EDUROAM AU MEMBERSHIP AND PARTICIPATION

3.1.1. The eduroam AU Member category "**IdP+SP Participant**" refers to the Institution operating as an eduroam IdP and SP. IdP+SP Participants MUST host their own RADIUS server and route eduroam authentication and user traffic to the internet via their subscribed AARNet service.

3.1.2. The eduroam AU Member category "**SP-Only Participant**" refers to the Institution operating as an eduroam SP only. SP-Only Participants MUST host their own RADIUS server. SP-Only Participants MAY route authentication and/or user traffic via their subscribed AARNet service, or via another Institution's subscribed AARNet service, or via another ISP.

3.1.3. AARNet is responsible for various functions, including operational auditing and monitoring, and other administrative functions as outlined in Appendix C.

4. EDUROAM AU MEMBER ROLES AND RESPONSIBILITIES

4.1 eduroam Identity Provider (IdP)

4.1.1. The IdP must comply with the Global eduroam Policy administrative and technical requirements for eduroam IdPs described in Appendix A.

4.1.2. The IdP MUST publish and require agreement by its users to comply with its institutional network acceptable use policy (AUP).

4.1.3. The IdP MUST configure its RADIUS server for mutual authentication by its user's client devices by validation of the IdP's RADIUS server x509 certificate and must make available the associated CA certificate if not automatically installed in client devices.

4.1.4. The IdP MUST enable its users to configure eduroam authentication locally and confirm successful authentication via eduroam prior to use of eduroam while travelling.

4.1.5. The IdP MUST provide information to users regarding end-user responsibilities for use of eduroam and MUST accept responsibility for the behaviour of their users (i.e. users they authenticate). The responsibilities communicated to users MUST include:

- The IdP's AUP must be complied with when accessing an SP's network via eduroam. The SP's AUP SHOULD be read. Where the IdP and SP AUPs differ or conflict, the more restrictive SHOULD apply. (A user not complying with a SP's AUP may be denied access by the SP and non-compliance notified to the user's IdP by the SP.) In the absence of an AUP, the general eduroam AU AUP (described in Appendix D) will apply.
- Configuration and confirmation of authentication via eduroam SHOULD be performed initially at the user's home institution (their IdP);
- Configuration of authentication by the IdP SHOULD enable mutual authentication (by user-device validation of the IdP RADIUS server certificate);
- User credentials SHOULD be securely issued, protected and not shared;

- Any loss or compromise of credentials, suspected or confirmed, SHOULD be reported to the IdP eduroam administrator promptly;
- Any faults or issues encountered in using eduroam SHOULD be reported to the IdP and/or the SP;
- User device security SHOULD be correctly maintained e.g. security patches applied and anti-virus measures in place. A device detected by the SP as exposing security vulnerabilities MAY be denied network access.

4.1.6. The IdP MUST have authority in taking appropriate action against its users in case of abuse reported by an SP, including denying an individual user's authentication via eduroam.

4.2 eduroam Service Provider (SP)

4.2.1. The role of the SP is to provide network access to a visitor as a result of the visitor's successful authentication via eduroam.

4.2.2 To ensure that users experience a reliable and high quality eduroam service globally, the SP SHOULD have high quality (low latency, high bandwidth) network management and access for guests. Membership of AARNet is RECOMMENDED but not essential and may not be available to any who do not meet AARNet's Access Policy requirement.

4.2.3. The SP MUST comply with the Global eduroam Policy administrative and technical requirements for eduroam SPs described in Appendix B.

4.2.4. The SP MUST publish its network access Acceptable Use Policy (AUP) and Privacy Policy for reference by visiting eduroam users.

4.2.5. Implementation of a dedicated VLAN for eduroam users that provides isolation from the SP's institutional network and tailoring of network access services is RECOMMENDED.

4.2.6. Implementation of a Quarantine VLAN enabling checking that the user device doesn't expose security vulnerabilities to the SP or other users of the SP's eduroam network is RECOMMENDED.

4.2.7. The SP MAY take appropriate action against users who do not comply with the SP's AUP, including denying network access and reporting the non-compliance to the user's IdP.

5. EDUROAM AU MEMBER SUPPORT

5.1 Deployment Information Maintenance

5.1.1. As eduroam is a global service, eduroam AU is responsible for providing accurate institutional deployment data to the global database.

5.1.2. Each Participant is responsible for administering their own deployment data in the AdminTool [2] (national eduroam database) which is managed by AARNet.

5.2 Support and Troubleshooting

5.2.1. The Institutions MUST provide end-user support and perform issue escalation as specified in Appendix A and B respectively of the Global eduroam Policy [1].

5.2.3. SPs MUST provide support to visitors from eduroam AU and global eduroam IdPs as required to access network services at the SP via eduroam.

5.2.4. The Institution's eduroam administrators MAY request support from AARNet eduroam staff in case of end-user or infrastructure issues that cannot be resolved locally.

5.2.5. The Institutions MUST cooperate with AARNet in performance of eduroam operability testing associated with providing end-user or institutional support.

5.3 Institutional Contacts

5.3.1. All Institutions MUST provide AARNet with contact details of at least two designated technical contacts. One of those contacts SHOULD be a group email address. Any changes to institutional contacts MUST be notified to AARNet in a timely manner.

6. AUTHENTICATION TRANSACTION AND NETWORK ACCESS LOGGING

6.1.1. All Institutions MUST log all authentication requests as specified in Appendix A and B.

6.1.2. Institutions MUST configure RADIUS servers to accurately record timestamps (e.g. configure to use NTP), and log timestamps is RECOMMENDED to be UTC.

6.1.3. All Institutions MUST notify users, via a dedicated eduroam webpage, that the IdP, SP and AARNet log user authentications.

6.1.4. Institutions MUST advise users, via a dedicated eduroam webpage, that SPs log network accesses and that such logs may be correlated with authentication transaction logs to allow a user's IdP to identify the user performing the network access.

6.1.5. Institutions MUST describe, via a dedicated eduroam webpage, how logs are stored and protected so as to comply with state or national legislation.

6.1.6. Institutions MUST restrict access to eduroam authentication transaction or network access logs to authorised staff. Logs MAY be disclosed to other Institutions and/or to AARNet in order to resolve Policy and/or AUP compliance issues, and to AARNet for eduroam AU operational purposes.

7. INSTITUTION EDUROAM WEBPAGES

7.1.1. Institutions MUST publish the following information via dedicated eduroam webpages:

(1) text that confirms best effort compliance with this document (including a link to this document published on the eduroam AU RO's website [3]);

(2) a link to the institution's network access AUP;

(3) the contact details for local eduroam support;

7.1.2. IdPs MUST publish the following information via dedicated eduroam webpages:

(1) recommendation for users to configure eduroam connectivity at their home institution;

(2) guidelines on eduroam username and password, and a summary of the eduroam authentication methods that may be used;

(3) platform specific device configuration guidelines (e.g. link to configuration scripts).

7.1.3. SPs MUST publish the following information via dedicated eduroam webpages:

(1) SSID used for eduroam (MUST be “eduroam” unless overlapping coverage requires use of an SSID of the form “eduroam-<abbreviated_institution_name>”;

(2) wireless encryption protocols supported (WPA2/AES MUST be supported);

(3) the eduroam coverage map;

(4) network services (protocol, ports, description) available to eduroam users and any restrictions or limitations in using the network.

APPENDIX A: ADMINISTRATIVE AND TECHNOLOGY COMPLIANCE FOR EDUROAM IDENTITY PROVIDERS

Copied from the Global eduroam Compliance Statement [1], Appendix A

A.1. eduroam IdPs MUST implement a RADIUS interface to connect to the eduroam infrastructure.

A.2. eduroam IdPs MUST implement an EAP method for all affiliated users that is suitable for wireless networks as well as wired, and supports mutual authentication and end-to-end encryption of credentials.

A.3. eduroam IdPs MUST send a RADIUS Access-Accept message for valid authenticated affiliated users for which they receive an Access-Request.

A.4. eduroam IdPs MUST send a RADIUS Access-Reject message for invalid users or those who are not authenticated.

A.5. eduroam IdPs MUST provide support to their users. Any support matters may be escalated to the RO or RC to coordinate and resolve.

A.6. eduroam IdPs MUST log all authentication attempts; the following information MUST be recorded:

- timestamp of authentication requests and corresponding responses
- the outer EAP identity in the authentication request (User-Name attribute)
- the inner EAP identity (actual user identifier)
- the MAC address of the connecting client (Calling-Station-Id attribute)
- the visiting SP for the user via the Operator-Name attribute, if present
- the visiting country of the request via the eduroam-SP-country attribute, if present
- type of authentication response (i.e. Accept or Reject).

The minimum retention time is three months, unless national regulations require otherwise.

APPENDIX B: ADMINISTRATIVE AND TECHNOLOGY COMPLIANCE FOR EDUROAM SERVICE PROVIDERS

Copied from the Global eduroam Compliance Statement [1], Appendix B

B.1. eduroam SPs networks MUST implement 802.1X with a RADIUS interface to connect to the eduroam infrastructure.

B.2. eduroam SPs IEEE 802.11 wireless networks MUST broadcast the SSID "eduroam". If there is more than one eduroam SP at the same location, an SSID starting with "eduroam-" MAY be used.

B.3. eduroam SPs IEEE 802.11 wireless networks MUST support WPA2+Enterprise (possibly via backwards compatibility).

B.4. eduroam SPs networks MUST provide IP address and DNS resolution auto-configuration infrastructure.

B.5. eduroam SPs networks SHOULD provide routable IP addresses, and MAY provide NAT translation.

B.6. eduroam SPs MUST forward all EAP-messages including outer identities, destined for eduroam participants, unmodified to the eduroam infrastructure.

B.7. eduroam SPs MUST NOT charge users or their eduroam IdPs for being admitted on the eduroam SP's access networks.

B.8. eduroam SP services are based on SP local policies. However, modifying the content of user connections (e.g., access lists or firewall filter rules to deny arbitrary ports or application-layer proxies) is strongly discouraged and MUST be reported to the respective RO.

B.9. eduroam SPs SHOULD keep sufficient logging information to be able to identify the responsible Identity provider for the logged-in user, by logging:

- timestamp of authentication requests and corresponding responses
- the outer EAP identity in the authentication request (User-Name attribute)
- the MAC address of the connecting client (Calling-Station-Id attribute)
- the MAC address and SSID of the connected access point (Called-Station-Id attribute, not always available)
- the SP identifier in the Operator-Name attribute (MAY be provided by the RO)
- type of authentication response (i.e. Accept or Reject)
- Chargeable-User-Identity (CUI attribute) if the IdP returns it.
- correlation information between a client's layer 2 (MAC) address and the layer 3 (IP) address that was issued after login if public addresses are used (e.g., DHCP logs)

The minimum retention time is three months, unless national regulations require otherwise.

APPENDIX C: EDUROAM AU ROAMING OPERATOR ROLES AND RESPONSIBILITIES

C.1 AARNet is responsible for complying with the Global eduroam Policy [1] on a "best efforts" basis.

C.2 AARNet is responsible for maintaining this document, ensuring it continues to satisfy Global eduroam Policy, and for promoting, monitoring and enforcing compliance by the Institutions.

C.3 AARNet's role is to deliver and maintain an eduroam AU National Infrastructure that allows the Institutions to securely share credential exchanges for authorised access with each other and with eduroam participants globally via Global eduroam infrastructure.

C.4 AARNet's eduroam AU operational goals include accomplishing the following tasks:

(1) define and implement a process enabling an eligible institution to join eduroam AU as an IdP+SP Participant and SP-Only Participant;

(2) define and implement an audit process to assess the Institution's operational compliance with this document. Performance of an operability audit may be requested by AARNet or by the Institution, at any time with a notification;

(3) the Institution define and implement delivery of eduroam AU usage metrics for the Institutions (generated from national server and/or institutional eduroam logs) and publish on a protected website;

(4) maintain Institution operability data and deployment information resources for eduroam AU and Global eduroam consumption in the format requested by the GeGC;

(5) capture, store securely and retain for a minimum of 6 months eduroam AU National RADIUS logs, including timestamp, user's outer identity, user's realm, user-device MAC address, SP server, authentication result, excluding user passwords;

(6) provide support to the Institutions via designated technical contacts, including expertise and guidance on the range of eduroam technology solutions deployed across eduroam AU;

(7) provide an issue tracking system which allows customer service requests to be submitted via email (support@aarnet.edu.au), facilitating request handling and customer interaction tracking;

(8) provide communication channel to ensure communications are delivered to the correct audience and to promote discussion on technical and policy topics;

(9) monitor security advisories and subscribe to technology mailing lists in order to identify security issues and advise the Institutions and require action as necessary to preserve the integrity and security of the eduroam service;

(10) maintain a dedicated eduroam AU website and publish eduroam AU service and operability information to the Institution administrators and end-users;

(11) publish information resources on deployment of eduroam at the Institutions, including links to information provided by Global eduroam;

(12) provide an eduroam deployment and promote the eduroam service at events and conferences;

(13) maintain involvement in eduroam AU community, working groups and committees;

(14) maintain links with the global eduroam community, including participation in the GeGC, and attendance at international meetings, conferences and events as required;

(15) provide direct assistance as required to national RO's in the APAN region, and participating and contributing to Global eduroam infrastructure and eduroam service resources for the APAN region;

(16) contribute to the further development of the eduroam service both nationally and globally.

APPENDIX D: GENERAL EDUROAM AU AUP

By using eduroam, Users agree to comply with the Acceptable Use Policies (AUPs) of both their home (IdP) and host (SP) institutions. IdPs and SPs AUPs must be readily available to Users. In the absence of an institutional AUP, the following rules apply:

- Users shall use eduroam responsibly and in a lawful manner.
- Users shall not use the service in ways that place NRO, your home institution (IdP), or host institution (SP) at risk.
- Users shall not
    - Launch attacks or engage in malicious activity.
    - Access or distribute illegal content (e.g. pirated software, copyrighted material).
    - Engage in fraud, phishing, or identity theft.
    - Attempt unauthorized access to systems or networks.
    - Spread malware, viruses, or other harmful software.
    - Send spam or bulk unsolicited messages.
    - Harass, threaten, or bully others online.
    - Share or collect personal data without consent.

- Misrepresent your identity or impersonate others.
- Use excessive bandwidth or disrupt network services.
- Circumvent network restrictions or firewalls.
- Share obscene, offensive, or discriminatory content.
- Violate any local or international laws.

Non-compliance with AUPs will result in revocation of User rights to use eduroam service.

REFERENCES

[1] eduroam Compliance Statement, Version2, Global eduroam Governance Committee

[2] AdminTool, What is the eduroam AU AdminTool? – AARNet Knowledge Base

[3] eduroam AU Policy – AARNet Knowledge Base

Version	**Date**	**Description**
1.0	28 August 2026	eduroam AU Process