eduroam AU Policy

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, terms & interpretation

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 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 is a "trust federation", with policy compliance on the basis of trust between an eduroam SP (institution providing network access) and an eduroam IdP (institution performing user authentication).

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

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

1.2. National eduroam and "eduroam AU"

1.2.1. eduroam **RO (Roaming Operator)** operates the national eduroam infrastructure that provides eduroam interoperability between eduroam SPs and IdPs at a national level.

1.2.2. Institutions participating in a National eduroam federation MUST comply with the National eduroam policy of the RO.

1.2.3. **"eduroam AU"** is the National eduroam federation for participating institutions in Australia.

1.2.4. **APL** (AARNet Pty Ltd) is Australia's national research and education network (NREN) provider and the eduroam AU RO.

1.3. Global eduroam

1.3.1. Institutions participate in eduroam globally (hereafter called **Global eduroam**) through their participation in a "National eduroam" federation.

1.3.2. Global eduroam is governed by the **Global eduroam Governance Committee (GeGC)**, which is coordinated by GÉANT (pan-European research and education network) and is comprised of representatives from Regional and National eduroam federations.

1.4. Global and National eduroam Policy

1.4.1. The GeGC's "**Global eduroam Compliance Statement**" [1] embodies the policy regarding

a National eduroam federation's participation in Global eduroam. It describes requirements and recommendations pertaining to a National eduroam RO's role and responsibilities.

1.4.2. National eduroam RO's MUST comply with "Global eduroam Compliance Statement" [1], hereafter referred to as the "**Global eduroam Policy**".

1.4.3. APL, the eduroam AU RO, is a signatory to the Global eduroam Policy.

1.4.4. This document, the "**eduroam AU Policy**", hereafter referred to as "**This Policy**", describes requirements and recommendations pertaining to an eduroam AU institutional participant's roles and responsibilities.

1.4.5. This Policy is intended to both satisfy the Global eduroam Policy requirements and to describe eduroam AU specific requirements and recommendations to facilitate achievement of APL's operational objectives for eduroam AU.

1.4.6. Appendices A and B of This Policy describe administrative and technical requirements for institutional participation in eduroam AU.

1.4.7. An eduroam AU institutional participant (hereafter referred to as "**The Institution**"or "**Participant**") MUST comply with This Policy.

1.5. Authority, Compliance & Policy Revision

1.5.1. APL and **CAUDIT (Council of Australian University Directors of Information Technology)** have joint responsibility for maintaining This Policy.

1.5.2. Revision of This Policy will be subject to APL and CAUDIT internal reviews and approvals.

1.5.3. The Institution's connection to the eduroam AU National Infrastructure operated by APL is interpreted as acceptance of This Policy by The Institution.

1.5.4. If APL identifies non-compliance with This Policy, APL 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, APL reserves the right to block The Institution's participation in eduroam.

1.5.5. In case of non-compliance where immediate action is deemed necessary by APL to protect the integrity and security of eduroam, APL 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.

1.5.6. The revised eduroam AU Policy will be released to all eduroam AU Participants. Participants will be provided a three months transition period to consider changes, seek clarification and provide feedback, and advise of their acceptance or lack of acceptance of the revised eduroam AU Policy.

1.5.7. During the transition period The Institutions are required to continue to comply with the incumbent policy unless the policy item is superseded by the revised policy in which case compliance with either is acceptable. By the conclusion of the transition period The Institutions MUST comply with the revised policy.

1.5.8. At the conclusion of the transition period, The Institutions which have notified lack of acceptance of the revised policy will be removed from eduroam AU participation.

1.5.9. In case of any event or behaviour constituting a threat to the security of eduroam, where immediate action is deemed necessary by APL to protect the security of Participants, APL reserves the right to suspend eduroam AU immediately and take appropriate action. If such a threat requires revision of This Policy, APL reserves the right to adopt a process with unspecified variation from that described by 1.5.2 to restore eduroam AU in a timely fashion.

1.6. eduroam Trademark and Logo

1.6.1. In accordance with the Global eduroam Policy, APL has registered the eduroam trademark and logo in Australia.

1.7. Further Information

1.7.1. A list of references and links to more information about eduroam is provided in Appendix D.

2. eduroam AU Membership and Participation

2.1. eduroam AU Member Categories

2.1.1. 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.

2.1.2. The eduroam AU Member category "**SP-Only Participant**" refers to The Institution operating as an eduroam SP only. SP-Only Participants MAY host their own RADIUS server or use RADIUS server provided by another Institution. SP-Only Participants hosting their own RADIUS server MAY connect to the eduroam AU National Infrastructure directly or via another institution's 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.

2.1.3. APL is responsible for providing support to eduroam AU members to achieve and maintain eduroam deployment and operability compliant with This Policy, including operational auditing and monitoring, other administrative functions as outlined in Appendix C.

2.2. Membership eligibility and rules: IdP+SP Participant

2.2.1. The Institution operating as an eduroam IdP SHOULD also operate as an eduroam SP. As the cost of network access is borne by the SP, the IdP+SP Participant justifiably expects reciprocity in terms of their users travelling to an IdP institution.

2.2.2. Eligibility for Membership of eduroam AU as an IdP+SP Participant is limited to institutions which are AARNet customers and have a current AARNet Access Agreement [2] in force and such AARNet customers' eligible users as defined under that Agreement.

2.2.3. IdP+SP Participants MUST comply with policy items (roles, responsibilities, operational requirements) described in This Policy for both eduroam IdPs and SPs.

2.2.4. New IdP+SP Participants MUST follow the eduroam AU joining process for IdP+SP Participants established and administered by APL.

2.2.5. IdP+SP Participants MUST bear the cost of any network access provided via eduroam by The Institution.

2.3. Membership eligibility and rules: SP-Only Participant

2.3.1. Eligibility for Membership of eduroam AU as an SP-Only Participant is open to any institution with a requirement, business case or other impetus for delivering network access to visitors from IdP+SP Participant institutions.

2.3.2. SP-Only Participants MUST comply with policy items (roles, responsibilities, operational requirements) described in This Policy for eduroam SPs.

2.3.3. New SP-Only Participants MUST follow the eduroam AU joining process for SP-Only Participants established and administered by APL.

2.3.4. eduroam AU SP-Only Participants MAY reach agreement with other Institutions (typically those IdP+SP Participants deriving benefit for their users) regarding cost recovery of network access provided via eduroam.

3. eduroam AU Member Roles and Responsibilities

3.1. eduroam Identity Provider (IdP)

3.1.1. The role of an eduroam identity provider is to authenticate users for whom it provides identity management and authentication credentials. Authentication of users via eduroam, enabling the user to access the SP's network, MUST comply with The Institution's acceptable use policy (AUP).

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

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

3.1.4. 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.

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

3.1.6. 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.)
- 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 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.

3.1.7. 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.

3.2. eduroam Service Provider (SP)

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

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

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

3.2.4. 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.

3.2.5. 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.

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

3.3. eduroam AU RO and Member Liability and Indemnity

3.3.1. To the extent permitted by law, neither APL nor any institution providing access to eduroam AU, shall be under any liability to any other institutions in respect of any loss, damage, cost or expenses whether arising under contract, tort (including negligence), statute or otherwise which may be incurred or suffered by that institution or its users arising out of the use of eduroam AU, including but not limited to any disruption to eduroam AU.

3.3.2. Neither APL nor any institution providing access to eduroam AU gives any warranties of any kind, whether express or implied, for or in relation to the suitability for any given purpose or purposes, or performance of eduroam AU, or that eduroam AU will be continuously available and excludes all implied warranties arising from a course of dealing, usage or trade practice.

4. eduroam AU Member Support

4.1. Deployment Information Maintenance

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

4.1.2. Each institution is responsible for administering their own deployment data in the Admintool (national eduroam database) which is managed by APL.

4.2. Operability Testing and Monitoring

4.2.1. IdPs MUST provide APL with an eduroam test account (username and password) for each of their realms to allow APL to authenticate via eduroam for the purpose of testing, auditing and monitoring of IdP operability. The test account username SHOULD contain the string "-test" to enable automatic removal of test account authentication transactions from usage reports. If the test account is disabled or the password is changed, the IdP MUST notify APL in a timely manner.

4.2.2. IdPs MUST configure APL's dedicated eduroam monitoring server as a trusted client in each of the IdP's RADIUS servers configured to authenticate its users to allow APL to issue authentication requests to each server for the purpose of testing, auditing and monitoring of IdP operability.

4.2.3. SPs MUST configure APL's dedicated eduroam monitoring server as a trusted client in each of the SP's RADIUS servers configured to forward authentication requests to the eduroam AU National Infrastructure to allow APL to issue authentication requests to each server for the purpose of testing, auditing and monitoring of SP operability.

4.3. Support and Troubleshooting

4.3.1. 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].

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

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

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

4.4. Institutional Contacts

4.4.1. The Institutions MUST provide APL with contact details of at least two designated technical contacts. One of those contacts SHOULD be a group email address.

4.4.2. The Institutions MUST provide APL with contact details of one designated security contact for notification of security issues; this MAY be the same person designated as a technical contact.

4.4.3. The Institutions MUST provide APL with contact details of one designated management contact for notification by APL of policy issues and notification of institutional non-compliance with This Policy or user non-compliance with AUPs.

4.4.4. Any changes to institutional contacts MUST be notified to APL in a timely manner.

4.4.5. The Institutions MUST have at least one technical contact subscribed to APL “eduroam participants” mailing list [5].

4.5. Authentication Transaction and Network Access Logging

4.5.1. The Institutions MUST log all authentication requests as specified in Appendix A and B.

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

4.5.3. Authentication transaction logs MUST NOT include user passwords.

4.5.4. The Institutions MUST notify users, via a dedicated eduroam webpage, that the IdP, SP and APL log user authentications.

4.5.5. The 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.

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

4.5.7. The 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 APL in order to resolve Policy and/or AUP compliance issues, and to APL for eduroam AU operational purposes.

4.6. Institution eduroam Webpages

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

(1) text that confirms best effort compliance with This Policy (including a link to This Policy published on the eduroam AU RO’s eduroam website);

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

(3) the contact details for local eduroam support;

(4) a link to the eduroam AU RO’s eduroam website.

4.6.2. 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) a link to the CA certificate required to validate the IdP server certificate;

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

4.6.3. 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.

4.7. Notifications and Alerts

4.7.1. Where APL issues a “security advisory” on the eduroam AU website and notifies The Institutions directly or via the eduroam mail list [5], The Institutions MUST comply and confirm by email to APL compliance with prescribed actions within 24 hours.

4.7.2. The Institutions MUST notify APL by email (support@eduroam.edu.au) within 24 hours of becoming aware of the following incidents:

(1) security breaches;

(2) misuse or abuse;

(3) authentication or access restrictions;

(4) service faults.

4.7.3. APL SHALL notify impacted institutions of any incidents, service interruptions or changes by email to The Institution’s designated eduroam support contact or to all The Institutions via the eduroam AU participant mail list [5].

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 routing fabric.

A.2. eduroam IdPs MUST implement an EAP method for all local 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 local users for which they receive an access request.

A.4. eduroam IdPs MUST NOT send a RADIUS access-accept 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)
- type of authentication response (i.e. Accept or Reject).

The minimum retention time is six 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+AES, and MAY additionally support WPA/TKIP as a courtesy to users of legacy hardware. Exceptionally, an SP established before January 1, 2012, MAY support only WPA/TKIP but not longer than January 1, 2013

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 SHOULD forward all EAP-messages, 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)
- type of authentication response (i.e. Accept or Reject)
- 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., ARP sniffing logs or DHCP logs)

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

Appendix C: eduroam AU Roaming Operator Roles and Responsibilities

C.1 APL is responsible for complying with the Global eduroam Policy [1] on a “best efforts” basis.

C.2 APL is responsible for maintaining This Policy, ensuring it continues to satisfy Global eduroam Policy, and for promoting, monitoring and enforcing compliance by The Institutions.

C.3 APL’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 APL’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 Policy. Performance of an operability audit may be requested by APL or by The Institution, at any time with a notification;

(3) define and implement an eduroam AU monitoring mechanism and process in order to provide real-time eduroam operability monitoring of The Institutions;

(4) 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;

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

(6) 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;

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

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

(9) provide mailing lists to ensure communications are delivered to the correct audience and to promote discussion on technical and policy topics;

(10) 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;

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

(12) publish generic eduroam configuration guidelines for standard platforms;

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

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

(15) maintain involvement in eduroam AU working groups and committees;

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

(17) 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;

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

Appendix D: Further Information

[1] Global eduroam Compliance Statement, Version 1.0, Global eduroam Governance Committee

[2] Policy on Allowed Access to AARNet, Version 1.4, AARNet Pty Ltd

[3] AARNet Pty Ltd provided eduroam AU website: www.eduroam.edu.au

[4] AARNet Pty Ltd supplied eduroam support email address: support@eduroam.edu.au.

[5] “AARNet PTY LTD” currently administers the following mailing list: Eduroam participants list - er-participants-l@lists.eduroam.edu.au;