

Australian eduroam® Policy
Version 2.0 (endorsed by CAUDIT on April 2 2007)

1.0 Background to this document

- 1.1 This document sets out guidelines that cover the control of the supply and receipt of Internet access for educational purposes, that is primarily (but not exclusively) offered to visitors of Participating Organisations within Australia.
- 1.2 eduroam is a TERENA registered trademark and is an abbreviation for “educational roaming” that originated from a European National Education and Research Networks (NRENs) project to deliver a user-friendly, secure and scalable internet access solution for visitors.
- 1.3 More information about eduroam is available at <http://www.eduroam.edu.au>

2.0 Roles and Responsibilities

2.1 CAUDIT

- 2.1.1 This policy and any future changes will be ratified by CAUDIT.

2.2 eduroam Service Provider (ESP)

- 2.2.1 AARNet are responsible for the ESP and will continue to utilize the management and technical skills and resources of Grangenet to deliver this service.
- 2.2.2 The ESP role is two fold, (1) to coordinate and support the eduroam service to nominated technical contacts of Participating Organisations only, and (2) to maintain links with the global eduroam community and their respective authentication servers, and contribute to the further development of the eduroam concept.
- 2.2.3 The ESP is responsible for maintaining and developing a national authentication server network that connects to Participating Organisations on a best efforts basis. The ESP assumes no liability for any impact as a result of a loss or disruption of service.
- 2.2.4 The ESP is responsible for managing a second line technical support function covering pre-connection and ongoing technical support and maintenance of a dedicated website containing technical, service, policy and process information¹, and mailing lists.
- 2.2.5 The ESP is responsible for coordinating communications between Participating Organisations so that policies and procedures contained herein are adhered to in a timely manner and as a matter of last resort has the right to impose technical sanctions.
- 2.2.6 The ESP will work with the nominated eduroam technical contact of a Participating Organisation to test one or more of the following aspects (1) initial connectivity, (2) authentication and authorisation processes and (3) the authorised services offered, and review of (1) the logging activities and (2) the relevant authentication server configuration for compliance with the policy.

2.3 Participating organisations: Home Organisation

¹ Handling security incidents, abuse of use, service faults, eduroam service blocking or shutdown/restart for operational or security reasons, including notifications thereof.

- 2.3.1 The role of the home organisation is to act as the credential provider for registered staff and students that must be over the age of 18 years of age or have parental consent to use this service. The role is to also act as the first line technical and service support function for its user's who want to access eduroam services at other Participating Organisations. Only nominated technical contacts can escalate technical support, service support or security issues on behalf of their users to the ESP.
- 2.3.2 The home organisation must abide by this policy and follow ESP service processes and guidelines listed herein and at <http://www.eduroam.edu.au> .
- 2.3.3 The home organisation is responsible for the behaviour of the users they authenticate and must take appropriate action in accordance with their local acceptable use policies (AUP) or equivalent where incidents of abuse are reported by visited organisations;
- 2.3.4 The home organisation must notify to their own users that Participating Organisations may log user activity.
- 2.3.5 There is an expectation that the home organisation will cooperate with ESP.

2.4 Participating organisations: Visited organisations

- 2.4.1 The role of the visited organisation is to supply internet access to visitors via eduroam (based on trusting that the visitor's home organisation authentication check and response is valid). The visited organisation has control over the authorisation of services.
- 2.4.2 Where user activity is monitored, the visited organisation must clearly announce this fact including how this is monitored, stored and accessed so as to comply with state or national legislation².
- 2.4.3 The visited organisation must abide by this policy and follow ESP service processes and guidelines listed herein and at <http://www.eduroam.edu.au> .
- 2.4.4 There is an expectation that the visited organisation will cooperate with ESP.

2.5 User

- 2.5.1 A user's role is in most cases as a visitor who wants internet access at another Participating Organisation. The user must abide by their home organisation AUP or equivalent and respect the visited organisation's AUP or equivalent. Where regulations differ and the user has been notified or instructed to do so, the more restrictive applies. For the avoidance of doubt, all users must as a minimum abide by relevant Australian law.
- 2.5.2 The user is responsible for taking reasonable steps to ensure that they are connected to a genuine eduroam service including adequate security checks (as directed by their home organisation) prior to entering their login credentials.
- 2.5.3 The user is responsible for their credentials and must not allow them or authorised internet access to be shared or used independently by other users.
- 2.5.4 If credentials may have been lost or compromised, the user must immediately report back to their home organisation.
- 2.5.5 The user is responsible for informing the visited organisation (where possible) and home organisation of any faults with the eduroam service.

² For example, to comply with the new NSW guidelines on workplace surveillance

- 2.5.6 The user is responsible for keeping their systems patched and uninfected with viruses, for example, otherwise access may be restricted by the visited organisation

3.0 Base service

- 3.1 Participating organisations must deploy an authentication server in accordance with eduroam technical and policy guidelines available at <http://www.eduroam.edu.au>. A secondary authentication server is recommended for resilience purposes.
- 3.2 The home organisation authentication server(s) must be reachable from the ESP authentication servers for authentication and accounting purposes.
- 3.3 The home organisation must create an eduroam test account (eduroam username and password credential) that will be made accessible to the ESP to assist in pre-connection testing, ongoing monitoring, support and fault finding activities. If the test account's password is changed, the ESP must be notified by the home organisation in a timely manner. No authorised services should be accorded to the test account.
- 3.4 The visited organisation may offer any media, however as a minimum, wireless LAN IEEE 802.11b is required whilst 802.11g is also recommended.
- 3.5 The Visited organisation must use "eduroam" as the SSID where there are NO instances of an overlap with other participant eduroam wireless hotspots. The SSID should be broadcasted and deployed with IEEE 802.1X Extensible Authentication Protocol (EAP) authentication (excluding EAP-MD5) to promote a consistent service and minimum level of security. If the "eduroam" SSID cannot be broadcasted due to technical limitations on the wireless access point, "eduroam" must be made available as a non-broadcasted SSID instead.
- 3.5.1 Where there are instances of an overlap with other participant eduroam wireless hotspots. All participating organisation must use a modified SSID name that must be no greater than 31 characters in length and must follow the "eduroam-institutional name" where the institution name is a shortened abbreviation of the full name.. It must also be a broadcasted SSID. This only applies to overlapping wireless hotspots operated by more than one participating organisation that results in users reporting an impact on access to authorized services. In these cases, all relevant participants must also inform the eduroam service provider responsible for the maintenance of the eduroam website so that service information to end users can remain up to date."
- 3.6 The visited organisation must as a minimum implement IEEE 802.1X and WPA/TKIP, or better.
- 3.7 The recommended access offered by the visited organisation is vpn, http, https, and ssh on both on net and off net however visited organisations may vary this access to meet with their requirements on the proviso that the services offered are publicised on both the visited organisation's eduroam web pages and on the <http://www.eduroam.edu.au> web site
- 3.8 Where the visited organisation chooses to offer access via off.net to authenticated users, the cost of access is charged to the visited organisation.
- 3.9 The visited organisation should implement a visitor VLAN for eduroam authenticated users that is not to be shared with other network services. The VLAN must use of publicly routable IPv4/IPv6 addresses using DHCP and should not use NAT for IPv4 addresses³.
- 3.10 The visited organisation is recommended to use Quarantine Virtual LANs that check the user device has up to date operating system and antivirus patches and no known viruses, prior to allowing authorised internet access.

³ NAT is discouraged because it could impact on current VPN services and future application services that may become available on eduroam.

- 3.11 The visited organisation must not charge for eduroam access. This service is based on a shared access model where Participating Organisations supply and receive Internet access for their users.

4.0 Logging

- 4.1 Participating organisations must log all authentication and accounting requests; the following information must be recorded

- (1) The date and time the authentication request was received;
- (2) The RADIUS request's identifier;
- (3) The authentication result returned by the authentication database;
- (4) The reason given if the authentication was denied or failed.
- (5) The value of the request's accounting status type.

- 4.2 The visited organisation must log all DHCP transactions; including

- (1) The date and time of issue of the client's DHCP lease;
- (2) The MAC address of the client;
- (3) The client's allocated IP address.

- 4.3 The visited organisation must keep a log of DHCP transactions for a minimum of three months. Access to these logs will be restricted to the eduroam technical contacts and ESP technical contact to assist in resolving specific security or abuse issues that have been reported to ESP.

5.0 Support

- 5.1 The home organisation must provide support to their users requesting access at a visited organisation campus.

- 5.2 The home organisation should provide support to users from other Participating Organisations that are requesting eduroam services at their home organisation campus.

- 5.3 The visited organisation must publish local information about eduroam services on dedicated web pages on their organisation website containing the following minimum information,

- (1) Text that confirms adherence (including a url link) to this policy document published on <http://www.eduroam.edu.au>;
- (2) A url link to visited organisation acceptable use policy or equivalent;
- (3) A list or map showing eduroam access coverage areas;
- (4) Details of the broadcasted or non-broadcasted SSID as eduroam;
- (5) A statement that eduroam is only available to users over 18 years of age or those users that have acquired parental consent to use the "non-filtered" Internet access;
- (6) Details of the authentication process and authorised services offered;
- (7) Details about the use of a non-transparent application proxy including user configuration guidelines (if applicable);
- (8) A url link to the <http://www.eduroam.edu.au> website and posting of the eduroam logo and trademark statement;
- (9) Where user activity is monitored, the visited organisation must clearly announce this fact including how this is monitored so as to meet with state or national legislation⁴, including how long the information will be held for and who has access to it.
- (10) The contact details of the appropriate technical support that is responsible for eduroam services.

6.0 Communications

⁴ For example, to comply with the new NSW guidelines on workplace surveillance

- 6.1 The home organisation must provide the ESP with contact details of two nominated technical contacts. Any changes to contact details must be notified to ESP in a timely manner.
- 6.2 The home organisation must designate a contact and their contact details to respond to security issues, this may be the same person designated as the nominated technical contact.
- 6.3 Participating organisation must have at least one nominated contact subscribed to the following mailing lists
- (1) Eduroam participants list - er-participants-l@lists.eduroam.edu.au.
 - (2) Eduroam policy list - er-policy-l@lists.eduroam.edu.au.
 - (3) Eduroam technical list (e.g. technical contact) - er-tech-l@lists.eduroam.edu.au.
 - (4) Eduroam site outage list (e.g. technical contact) - er-outage-l@lists.eduroam.edu.au.
 - (5) Eduroam abuse list (security contact only) - er-abuse-l@lists.eduroam.edu.au.
- 6.4 Participating organisations must notify the ESP in a timely manner of the following incidents; (1) security breaches; (2) misuse or abuse; (3) service faults; (4) changes to access controls (e.g. permit or deny of a user or realm)

7.0 Authority, Compliance & Sanctions

- 7.1 The authority for this policy is the ESP who will implement this policy.
- 7.2 Any changes to this policy will be made in consultation with Participating Organisations and CAUDIT.
- 7.3 Connecting to the ESP authentication servers will be deemed as acceptance of this policy. Any organisation that is currently connected will be given a period of one month's grace from the official ratification date of this policy by CAUDIT, to either continue to connect as a statement of acceptance of this policy or the removal of their authentication server connection(s) to indicate an inability to accept this policy at the present time.
- 7.4 In cases where immediate action is required to protect the integrity and security of the eduroam service, the ESP has the right to suspend the eduroam service or restrict eduroam access to only those Participating Organisations that can comply with the required changes. To do so, the ESP will notify Participating Organisations of such incidents, outages and remedial action to be taken on the er-outage-l@lists.eduroam.edu.au mailing list.
- 7.5 The ESP will notify by email to the nominated technical and/or security contact of the Participating Organisation of any technical or policy breach or incident that requires resolution. Where such notifications are not acted upon in a timely manner, or where the breach or incident may impact on the security and integrity of eduroam, the ESP has the right to block eduroam access to that organisation.
- 7.6 Visited organisations may prevent use of their networks by all users from a particular home organisation by configuring their authentication server(s) to reject that realm; in some cases a visited organisation may also be able to block a single visiting user.
- 7.7 Home organisations may withdraw an individual user's ability to use the eduroam by configuring their own authentication server or removing that user from their authentication database.
- 7.8 Home organisations must also ensure that their computing regulations enable users who breach this policy to be subject to an appropriate internal disciplinary process irrespective of their location at the time.