REANNZ

policy

NAME	New Zealand eduroam policy
DATE	13 August 2013

1 Introduction

1.0.1. Research and Education Advanced Network New Zealand Ltd (REANNZ) aims to foster collaboration between education and research organisations in New Zealand and globally. Facilitating the provision of roaming network access through the federated eduroam service ("the service") is a major component in the fulfilment of this aim and is governed in New Zealand by REANNZ.

1.0.2. This document sets out guidelines that cover the control of the supply and receipt of Internet access for educational and research purposes, that are primarily (but not exclusively) offered to visitors of Participating Organisations within New Zealand.

1.0.3. eduroam is a TERENA registered trademark and is an abbreviation for "educational roaming." It originated from a European National Education and Research Network's (NRENs) project to deliver a user-friendly, secure and scalable Internet access solution for visitors.

1.0.4. More information about eduroam is available at www.eduroam.org

2 Roles and Responsibilities

2.1. REANNZ

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

2.1.2. Terminology in this document follows the terminology definitions provided in the eduroam Compliance Statement v1.0 (4 October 2011) unless specifically stated in this document.

2.2. eduroam Roaming Operator (RO)

2.2.1. REANNZ is the RO for New Zealand and is responsible for delivering the eduroam service to Participating Organisations in New Zealand.

2.2.2. The RO's role is to:

- To coordinate and support the eduroam service to nominated technical contacts of Participating Organisations only
- Maintain links with the global eduroam community and their respective authentication servers
- Contribute to the further development of the eduroam concept.

2.2.3. The RO is responsible for maintaining and developing a national authentication server network that connects to Participating Organisations on a best efforts basis. The RO assumes no liability for any impact as a result of a loss or disruption of service.

2.2.4. The RO 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 information and mailing lists.

2.2.5. The RO is responsible for coordinating communications between Participating Organisations so that policies and procedures contained herein are adhered to in a timely manner. As a matter of last resort the RO has the right to impose technical sanctions.

2.2.6. The RO will work with the nominated eduroam technical contact of a Participating Organisation to test one or more of the following aspects:

- initial connectivity
- authentication and authorisation processes
- the authorised services offered
- review of the logging activities
- review of the relevant authentication server configuration for compliance with the policy.

2.3. Participating Organisations: eduroam Identity Provider (IdP)

2.3.1. The role of the IdP is to act as the credential provider for registered staff and students of that organisation. IdPs also act as the first line technical and service support function for its users 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 RO.

2.3.2. The IdP must abide by this policy and follow RO service processes and guidelines listed herein and at www.reannz.co.nz/eduroam.

2.3.3. The IdP 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 eduroam Service Providers.

2.3.4. The IdP must notify to their own users that Participating Organisations may log user activity.

2.3.5. There is an expectation that the IdP will cooperate with the RO.

2.4. Participating Organisations: eduroam Service Provider (SP)

2.4.1. The role of the SP is to supply Internet access to visitors via eduroam (based on trusting that the visitor’s IdP authentication check and response is valid). The SP has control over the authorisation of services.

2.4.2. Where user activity is monitored, the SP must clearly announce this fact including how this is monitored, stored and accessed so as to comply with any legislative requirements.

2.4.3. The SP must abide by this policy and follow RO service processes and guidelines listed herein and at www.reannz.co.nz/eduroam.

2.4.4. There is an expectation that the SP will cooperate with the RO.

2.5. User

2.5.1. A user’s primary role will be as a visitor who requires Internet access at another Participating Organisation. The user must abide by their IdP’s AUP or equivalent and respect the SP’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 New Zealand legislation.

2.5.2. The user is responsible for taking reasonable steps to ensure that they are connected to a genuine eduroam SP including adequate security checks (as directed by their IdP) 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 IdP.

2.5.5. The user is responsible for informing the SP (where possible) and IdP of any faults with the eduroam service.

2.5.6. The user is responsible for keeping their systems patched and protected with suitable anti-virus/malware protection otherwise access may be restricted by the SP.

3 Service Definition

3.1. Base service

3.1.1. Participating Organisations must deploy an authentication server in accordance with the eduroam technical and policy guidelines available at www.reannz.co.nz/eduroam. A secondary authentication server is recommended for resilience purposes.

3.1.2. The IdP authentication server(s) must be reachable from the RO authentication servers for authentication and accounting purposes.

3.1.3. The IdP must create an eduroam test account (eduroam username and password credential) that will be made accessible to the RO to assist in pre-connection testing, ongoing monitoring, support and fault finding activities. If the test account's password is changed, the RO must be notified by the IdP in a timely manner. No authorised services should be accorded to the test account.

3.1.4. The SP may offer any media; however an IEEE 802.11 based wireless LAN is typically expected. Where the SP offers wireless LAN access, the SP should ensure they offer a network that continues to meets current best-practice wireless standards.

3.1.5. The SPs IEEE 802.11 wireless networks must broadcast the SSID "eduroam" (all in lowercase) as the wireless SSID where there are no instances of an overlap with other SP.

3.1.6. Where there are instances of an overlap with other SP eduroam wireless hotspots, Participating Organisations must use a modified broadcast 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. This only applies to overlapping wireless hotspots operated by more than one Participating Organisation that results in users reporting an impact on access to authorised services. In these cases, all relevant SPs must also inform the RO so that service information available to end users can remain up to date.

3.1.7. The SP must as a minimum implement IEEE 802.1X and WPA2/AES or better. The SP may optionally support WPA/TKIP, though its use is discouraged due to published cryptographic weaknesses.

3.1.8. The recommended minimum access offered by the SP is vpn, http, https, and ssh for both on and off net destinations. However SPs may vary this access to meet with their requirements on the proviso that the services offered are publicised on both the SP’s eduroam web pages and on the REANNZ website.

3.1.9. Where the SP chooses to offer access to off net destinations to authenticated users, the cost of access is covered by the SP.

3.1.10. The SP should implement a visitor VLAN for eduroam authenticated users that is not to be shared with other network services. The VLAN should use publicly routable IPv4/IPv6 addresses where possible and should avoid the use of NAT for IPv4 addresses. A DHCP server must be provided to allocate IPv4 addresses.

3.1.11. The SP is recommended to either use Quarantine VLANs that check the user device has up to date operating system and antivirus patches and no known viruses prior to allowing authorised Internet access, or actively monitor the eduroam VLAN for infected and/or compromised user devices and pre-emptively remove network access to a user device that is detected to be attempting to infect or attack other devices.

3.1.12. The SP 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.

3.2. Logging

3.2.1. The IdP must log all authentication requests; the following information as a minimum must be recorded:

- The 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).

3.2.2. eduroam SPs should keep sufficient logging information to be able to identify the responsible IdP for the logged-in user, by logging:

- The 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 type of authentication response (i.e. Accept or Reject)
- The 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).

3.2.3. Participating Organisations must keep the above logs for a minimum of six months.

3.2.4. Access to these logs will be restricted to the eduroam technical contacts and RO technical contact, or relevant staff responsible for maintaining and supporting these logs as per the visited organisation policy, to assist in resolving specific security or abuse issues that have been reported to RO.

3.3. Support

3.3.1. The IdP must provide support to their users requesting access at a remote SP.

3.3.2. The SP should provide support to users from other IdPs that are requesting eduroam services.

3.3.3. The SP must publish local information about eduroam services on dedicated web pages on their organisation website containing the following minimum information:

- Text that confirms adherence (including a URL link) to this policy document published on www.reannz.co.nz/eduroam
- A URL link to SP acceptable use policy or equivalent
- A list or map showing eduroam access coverage areas
- Details of the authentication process and authorised services offered
- Details about the use of a non-transparent application proxy including user configuration guidelines (if applicable)
- A URL link to the www.reannz.co.nz/eduroam website and posting of the eduroam logo and trademark statement

- Where user activity is monitored, the SP must clearly announce this fact including how this is monitored so as to meet with any applicable legislation, including how long the information will be held for and who has access to it
- The contact details of the appropriate technical support that is responsible for eduroam services.

3.4. Communications

3.4.1. The IdP must provide the RO with contact details of two nominated technical contacts. Any changes to contact details must be notified to RO in a timely manner.

3.4.2. The IdP 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.

3.4.3. Any Participating Organisation must have at least one nominated contact subscribed to the following mailing lists:

- Operators, eduroam-ops@reannz.co.nz
- Announcements, eduroam-announce@reannz.co.nz

3.4.4. Participating Organisations must notify the RO in a timely manner of the following incidents:

- Security breaches
- Misuse or abuse
- Service faults
- Changes to access controls (e.g. permit or deny of a user or realm).

4 Legal

4.4.1. The authority for this policy is the RO who will implement this policy.

4.4.2. Any changes to this policy will be made in consultation with Participating Organisations and REANNZ.

4.4.3. Connecting to the RO 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 REANNZ, 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.

4.4.4. In cases where immediate action is required to protect the integrity and security of the eduroam service, the RO 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 RO will notify Participating Organisations of such incidents, outages and remedial action to be taken on the eduroam-announce@reannz.co.nz mailing list.

4.4.5. The RO 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 RO has the right to block eduroam access to that organisation.

4.4.6. SPs may prevent use of their networks by all users from a particular IdP by configuring their authentication server(s) to reject that realm; in some cases a SP may also be permitted to block a single visiting user. If these measures are deployed, this must be notified to the RO.

4.4.7. IdPs 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.

4.4.8. IdPs 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.