**eduroam at *Institution***

*This document is intended to be read by both visitors to Institution’s offices, and also by Institution staff who intend to use eduroam to connect to visited institution’s Wi-Fi networks.*

**What is eduroam?**

eduroam is short for "education roaming".

eduroam is a global service enabling staff and students of educational, research and related institutions to visit another eduroam participating institution and connect to the visited institution's wireless network automatically, i.e. with minimal effort for both user and visited institution.

Eduroam infrastructure provided by *Institution* and global participants enables an *Institution* visitor's 'home institution' to authenticate the visitor remotely. Upon successful authentication, *Institution* grants wireless network access to the visitor. Other eduroam participating institutions similarly grant network access to *Institution* staff visiting those institutions.

If configured correctly, eduroam users, either visitors to *Institution* sites, or travelling *Institution* staff, should be able to get an eduroam connection at a visited institution just by opening their laptop or activating their phone or other mobile device.

[More about eduroam](http://www.eduroam.edu.au/) is available from AARNet’s eduroam AU website, which AARNet publishes as part of its responsibilities in its role of the eduroam AU ‘roaming operator’.

**eduroam Policy**

Trust in eduroam authentication is underpinned by use of a proven secure technical infrastructure and protocol, and a set of policies to which all eduroam participants are required to comply.

In participating in eduroam AU, *Institution* agrees to conform to the [Global eduroam Policy](http://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf) and the [eduroam AU national policy](https://support.aarnet.edu.au/hc/en-us/article_attachments/360000514475/eduroam-national-policy_v4.2.pdf) maintained by *Institution*.

**What is the users' responsibility in using eduroam?**

The eduroam AU policy states that eduroam users must conform to their home institution's network Acceptable Use Policy (AUP).

Users are recommended to read and comply with the Acceptable Use Policy of visited institutions. Visiting eduroam users should refer to [*Institution AUP*](http://www.institution.edu.au/aup).

If non-compliant activities are reported to the user’s home institution by a visited institution, the home institution is required to take action against the user as would occur if the activity had occurred on the home institution network.

User activity logs are captured in order to enable the institution providing the eduroam network to track the end user with the help of their home institution.

**Is eduroam secure?**

eduroam protocols prevent your institutional password from being revealed to any eduroam server other than your home institution’s eduroam server. So your login password is protected and remains secret between you and your home institution.

**What about user privacy?**

Your eduroam username is visible to the Institution’s institutional RADIUS server and other eduroam infrastructure servers involved in getting your authentication request from your device to your home institution. Your username and your device MAC address are recorded in logs of each RADIUS server involved in proxying your authentication request to your home institution.

**Institution’s Wireless Settings**

|  |  |
| --- | --- |
| SSID (Network Name)  | eduroam |
| Wireless Network Connection Protocol  | WPA2 Enterprise  |
| Data Encryption Method  | AES  |

***Institution* Users using Eduroam**

*Institution* users should configure eduroam authentication locally (i.e. while on *Institution* campus) and confirm successful authentication by *Institution* eduroam infrastructure before travelling to other eduroam participating institutions.

**Authentication Configuration**

The following authentication parameters apply to authentication of *Institution* students and staff via eduroam *(below assumes the realm is institution.edu.au)*:

|  |  |
| --- | --- |
| Security | WPA2-Enterprise |
| Encryption | AES |
| EAP Method | PEAP |
| Inner Method | MSCHAPV2 |
| Identity | < Institution username>@Institution.edu.au |
| Anonymous Identity | Do not configure an anonymous identity |
| CA Certificate | Will auto-detect |

**User Device Configuration**

Device configuration scripts are available from the eduroam Configuration Assistant Tool (eduroam CAT).

In order to download scripts from the eduroam CAT,

1. Visit <https://cat.eduroam.org/>

2. Click on link labelled: "Click here to download your eduroam installer"

3. Select Organisation: *Institution*

4. Download appropriate script for your mobile device, following instructions obtained by

clicking on the [i] button to read information related to your installer.

E.g. if you are using an Apple mobile phone or other Apple iOS mobile device, the information link will contain the following information:

For best results, please use the built-in browser (Safari) to open the configuration file.

The profile will install itself after you click (or tap) the button.

You will be asked for confirmation/input at several points:

\* to install the profile

\* to accept the server certificate authorities (2 times)

\* to enter the username and password you have been given by your organisation

5. Follow instructions to install the authentication configuration script. Note if you have an eduroam configuration already, you should “forget” the connection or delete the existing profile.

**Note:** Manual authentication configuration of devices is not recommended, as use of the CAT scripts ensures you are configured according to security best practices, and ensures an understood, consistent configuration in case you require support in using eduroam.

*If you have trouble installing the script, or if there is no script available on the eduroam CAT for your mobile device, please request support via Institution’s service desk support@institution.edu.au.*

**Visitors using eduroam at *Institution***

**Who can use eduroam at *Institution*?**

eduroam is available to general staff, academics, researchers and students from eduroam participating educational, research and related institutions globally.

**How do I use eduroam at *Institution*?**

**Note:** As an eduroam user, you should have already configured access to eduroam while on your home campus, using the authentication parameters provided by your home institution local eduroam webpage.

The wireless encryption protocol used by *Institution* access points is the Wi-Fi standard "WPA2/AES" (also called WPA2 Enterprise). Accessing eduroam successfully within *Institution* requires only that your device’s configured wireless network connection and encryption protocol is compatible. Due to near-ubiquity of "WPA2/AES" support by institutional wireless access points, it is pretty much guaranteed that your wireless connection will be configured correctly if you’ve already tested your eduroam authentication on your own campus.

**Note:** There is no need to change any of your authentication parameters. These are only relevant to your home institution. If you have successfully configured authentication to eduroam at your home institution, you should be able to access *Institution* campus's network via eduroam with no change to your setup.

**Where exactly can I use eduroam within *Institution*?**

Institution provides eduroam at each of its office locations listed at [*https://www.institution.edu.au/locations*](https://www.institution.edu.au/locations)

* *Sydney*
* *Canberra*
* *Melbourne*
* *Brisbane*
* *Perth*
* *Adelaide*
* *Hobart*

**Network Services Provided**

*Institution* provides full outbound access with NAT’ed IP addresses. In other words, you can access any services you normally do e.g. the Internet, your institution via VPN etc. However any servers running on your devices will not be accessible externally while connected to the *Institution* network.

**How do I get support in using eduroam?**

When you're on an *Institution* campus and connect to eduroam, due to relative complexity of wireless and eduroam infrastructures, you may experience difficulty in getting a network connection due to several reasons e.g. an issue with your device configuration, wireless networking, institutional eduroam operability or eduroam infrastructure operability.

If network access issues occur, if practicable, in the first instance eduroam users should **contact their home institution's IT helpdesk** to seek support.

If this is not possible, or if the home institution can’t resolve the issue, visiting users should seek help from an *Institution* staff member or contact the Institution IT support via *support@institution.edu.au**.*

If required, your home institution's or *Institution* eduroam support staff will contact *Institution’s* eduroam AU national administrator for additional assistance.

**What Usage Logs are kept by *Institution* and what are they used for?**

The eduroam trust model (between institutions remotely authenticating their users, and other institutions providing network access, via eduroam) is supported by the ability to trace a particular network access event to an authentication of a 'real user' by their home institution.

Home institutions agree to take appropriate action on behalf of visited institutions in case a user doesn’t comply with the home institution’s network AUP.

In order to provide this traceability, remote authentication and network access transactions via eduroam are logged by *Institution*, with logs being retained for a period of six months. Access to usage logs is restricted to authorised personnel and authorities as required by the law.

Usage logs may also be used for purposes of service trouble-shooting and user support.