



eduroam AU AdminTool Institutional Administrator Guide

Author: Neil Witheridge

Date: 5th June 2020

Version: 1.0

About This Guide

This guide describes the eduroam AU institutional administrator's required usage of the eduroam AU AdminTool.

Following administrator registration for an eduroam participating institution, and activation of that administrator account by the national roaming operator (NRO i.e. AARNet), the institutional administrator is required to keep the institution's eduroam deployment data up to date.

This data is used to create an XML file which is consumed (on a daily basis) by the eduroam Global Database. This in turn provides global eduroam participation information to all national roaming operators.

A public interface is also provided by the eduroam AdminTool which provides information to end-users. In particular, the institution's network Acceptable Use Policy is important to make readily available to end-users.

Contents

Overview	2
Access via SAML Authentication	2
Administrator Registration and Activation	3
Populating eduroam Deployment Data	4
Institution Data.....	4
Editing Insitution Data	5
Location Data	6
Adding a new location	7
Server Data	8
Adding a New Server	8
Realm Data.....	9
Edit Action	9
Add new realm.....	9
Monitoring Data	10
Edit Monitoring Action	10
Edit Monitoring Account Parameters.....	11
Add Monitored Realm.....	11
Contacts Data.....	12
Edit Contact Account Action.....	12
Add New Contact	12
XML File Provided to Global Database	13

Overview

The purpose of the eduroam AU AdminTool is to enable up-to-date information about eduroam AU deployment to be made available to the national roaming operator (AARNet), to end-users, and to the eduroam global database.

It is the responsibility of eduroam AU participant institutions to maintain the accuracy of their data. Nominated institutional administrators are granted access to enter their institutional eduroam deployment data.

Institutions are advised that a subset of data entered into the AdminTool is shared globally (refer to the XML file section of this document).

Note that no security sensitive information is stored in the AdminTool. The fields for RADIUS server secrets and institutional test account passwords are locked and only a default value is stored in the AdminTool database.

Access via SAML Authentication

The “Manage” menu item of the AdminTool provides access to the institutional administrator pages.

Institutional Administrators access the AdminTool via their SAML IdP or via the AAF Virtual Home Organisation.

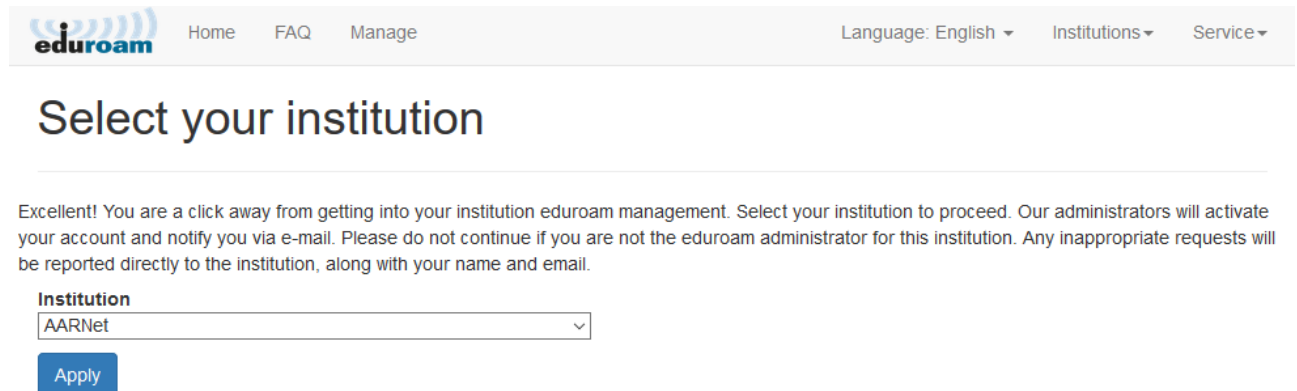
SAML Access is provided via the AARNet OpenConext instance, a SAML IdP-SP proxy.

The screenshot displays the eduroam AU AdminTool interface. At the top, there is a navigation bar with 'Home', 'FAQ', and 'Manage' (the 'Manage' link is circled in red). To the right of the navigation bar are links for 'Language: English', 'Institutions', and 'Service'. Below the navigation bar is a map of Australia and New Zealand. The map shows various regions with blue cloud icons and numbers indicating deployment locations. The map includes labels for 'Jakarta', 'Jawa Sea', 'Banda Sea', 'Arafura Sea', 'Salomon Sea', 'Tasman Sea', 'Coast Sea', 'Auckland', 'Wellington', and 'Christchurch'. Below the map is a 'Login' section with logos for Shibboleth, DJ NRO, and Google.

Refer to the eduroam website page describing the AARNet conext authentication service.

Administrator Registration and Activation

The first time an institutional administrator accesses the service via SAML, a prompt appears allowing nomination of the institution they wish to administer.

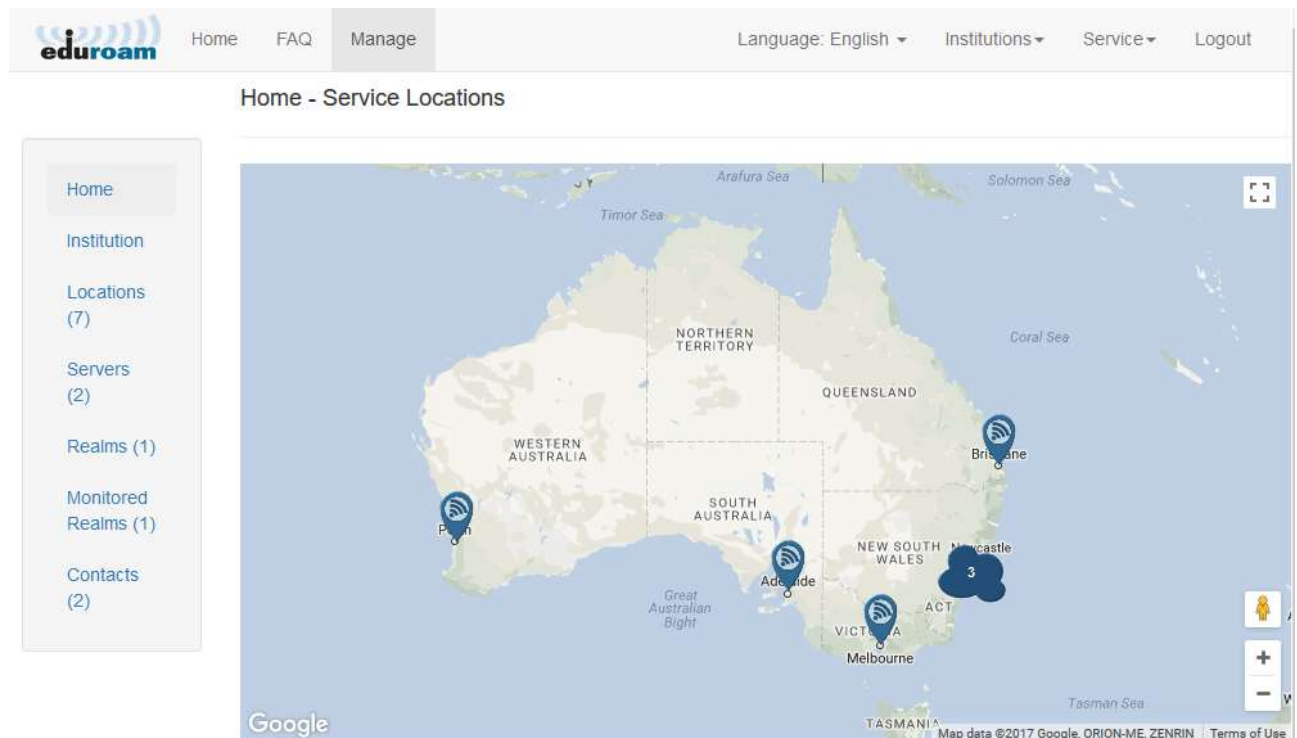


An email is sent to the NRO administrator who is responsible for activating the institutional administrator for the nominated institution.

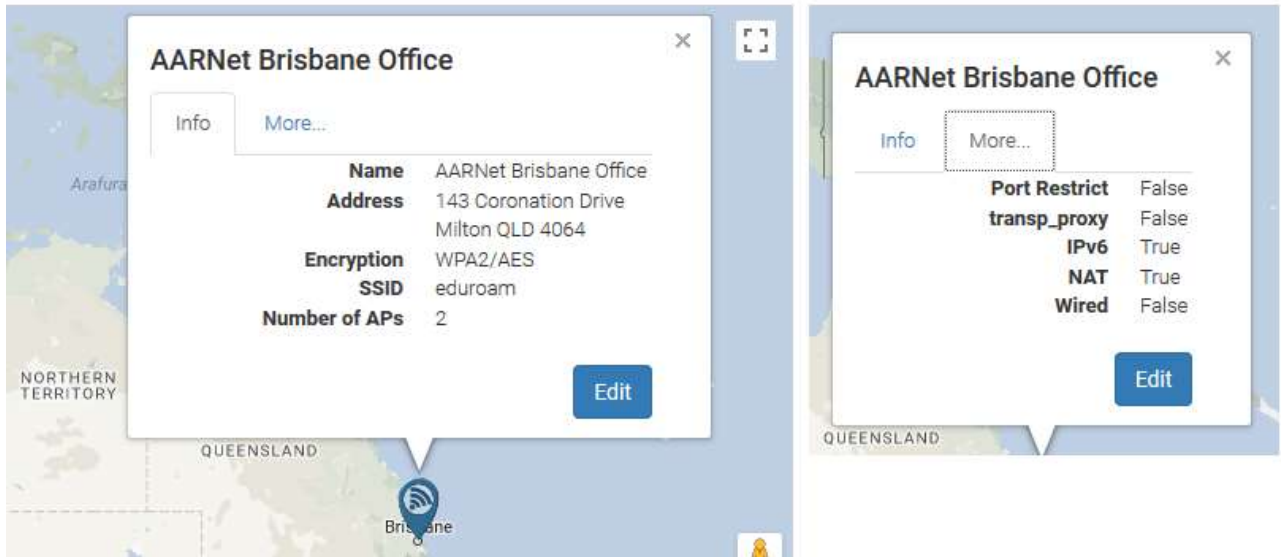
Once activated, a confirmation email is sent to the administrator.

The administrator can then access the AdminTool via the Manage menu item and will either see a page indicating this institution has no data and needs to be populated from scratch, or displays existing details for the institution.

For example, when the AARNet institutional administrator logs into the AdminTool, a map will be displayed showing already configured locations.



Information already entered for each location can be displayed by pressing on the eduroam location icons

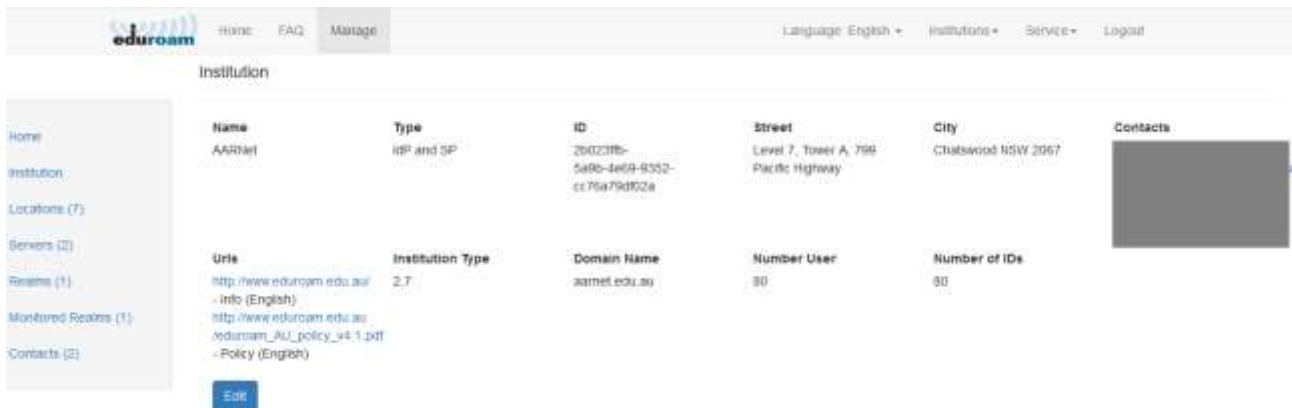


Populating eduroam Deployment Data

The primary role of the eduroam AU is to maintain up-to-date institutional eduroam deployment data. The following categories of data are required to be entered.


Institution Data

Basic information about the institution.



The “Number User” and “Number of IDs” are rough estimates only.

Editing Insitution Data


Home FAQ Manage

Language: English ▾
Institutions ▾
Service ▾
Logout

AARNet Edit

- Home
- Institution
- Locations (7)
- Servers (2)
- Realms (1)
- Monitored Realms (1)
- Contacts (2)

Name

Type

ID

Address

Street	City	Language
<input type="text" value="Level 2 Building 1, Bini"/>	<input type="text" value="North Ryde NSW 211"/>	<input type="text" value="English"/> Remove

Add Another

Contacts

Add

Uris

url	type	language
<input type="text" value="http://www.eduroam.edu.au/"/>	<input type="text" value="info"/>	<input type="text" value="English"/> Remove
<input type="text" value="http://www.eduroam.edu.au/"/>	<input type="text" value="Policy"/>	<input type="text" value="English"/> Remove

Add Another

Institution Type

IEEE 802-11-2012, clause 8.4.1.34 Venue info. This is a pair of integers, each between 0 and 255, separated with ".".

Domain Name

The primary, registered domain name for your institution, eg. example.com. This is used to derive the Operator-Name attribute according to RFC5580, par.4.1, using the REALM namespace.

Number of Users

Number of users (individuals) that are eligible to participate in eduroam service

Number of IDs

Number of issued e-identities (credentials) that may be used for authentication in eduroam service


Apply

If you have any questions or need help, contact Domain Helpdesk (helpdesk@example.com) - 12324567890
 This is a service provided by AARNet.
 Powered by [DINRO](#) v1.2.1

Location Data

It is important that globally eduroam users know where eduroam access is available, i.e. where the “eduroam” SSID is broadcast.

Location information is intended to provide information on locations and also any differences to the wireless service at these sites.


Home FAQ **Manage**
Language: English ▾ Institutions ▾ Service ▾ Logout

Locations

- Home
- Institution
- Locations (7)
- Servers (2)
- Realms (1)
- Monitored Realms (1)
- Contacts (2)

Display locations
Search:

Name	Address	SSID	Encryption Level	AP no	Actions
AARNet Sydney - UTS	15 Broadway, Ultimo (Level 10, Building 1 UTS) Ultimo NSW 2007	eduroam	WPA2/AES	2	edit delete
AARNet Perth Office	20 Dick Perry Avenue Kensington WA 6151	eduroam	WPA2/AES	2	edit delete
AARNet Melbourne Office	62 Lygon Street Carlton South VIC 3053	eduroam	WPA2/AES	2	edit delete
AARNet Head Office	799 Pacific Highway Chatswood NSW 2067	eduroam	WPA2/AES	2	edit delete
AARNet Canberra Office	Building 9, Banks Street Yarralumla ACT 2600	eduroam	WPA2/AES	2	edit delete
AARNet Brisbane Office	143 Coronation Drive Milton QLD 4064	eduroam	WPA2/AES	2	edit delete
AARNet Adelaide Office	Mawson Lakes Blvd (Room E1-18 Building E UniSA) Mawson Lakes SA 5095	eduroam	WPA2/AES	2	edit delete

Showing 1 to 7 of 7 entries
← Previous **1** Next →


+ Add a new location

Adding a new location

Add Location

- Home
- Institution
- Locations (7)
- Servers (2)
- Realms (1)
- Monitored Realms (1)
- Contacts (2)

Location



Search location

Lat

Longitude in decimal degrees, up to 8 decimal places

Lng

Latitude in decimal degrees, up to 8 decimal places

ID

Stage

Location Name

Name	Language	
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>

Address

Street	City	Language
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>

Contacts

<input type="text"/>

Physical Availability

Restrictions regarding physical access to the service area.

Operation Hours

Free text description of opening hours, if service is not available 24 hours per day

Location Type

IEEE 802.11-2012, clause 8.4.1.34 Venue Info. This is a pair of integers, each between 0 and 255, separated with ".".

SSID

Encryption Level

- WPA-TKIP
- WPA-AES
- WPA2-TKIP
- WPA2-AES
- WPA3-AES

AP number

Wired number

Tags

- port restrictions
- transparent proxy
- IPv6
- NAT
- Passpoint (Hotspot 2.0)

Urls

url	type	language	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>

If you have any questions or need help, contact Domain Helpdesk (helpdesk.example.com) - 12324567890
 This is a service provided by AARNet
 Powered by DJNRO v1.2.1

Server Data

RADIUS servers can be configured to operate as “Service Providers”, proxying all requests to the National RADIUS Servers, or as Identity Providers, authenticating local realms.

The screenshot displays the 'Servers' management interface. At the top, there is a navigation bar with 'Home', 'FAQ', and 'Manage' tabs. Below this, a search bar and a table of servers are visible. The table has columns for Name, Type, Authentication Port, Protocol, and Action. Two servers are listed: 'aarnet.edu.au-3' and 'aarnet.edu.au-2', both with Type 'IdP and SP', Authentication Port '1812', and Protocol 'radius'. Each server entry has 'edit' and 'delete' buttons. Below the table, there are pagination controls showing 'Showing 1 to 2 of 2 entries' and an 'Add new server' button.

Adding a New Server

Add Server

Type

Address Family

Hostname

 IP address | FQDN hostname

Label

 Descriptive label

RADIUS Packet Types

Authentication Port

 Default for RADIUS: 1812

Accounting Port

 Default for RADIUS: 1813

Status-Server

 Do you accept Status-Server requests?

Secret

 Do not enter secret
 Secret is not stored currently

Protocol

Realm Data

For Identity Provider participants, the institutional realms supported will include at least the primary domain (with an appended “.au” country code DN component if the primary domain doesn’t include it).

Note that only under rare exceptional circumstances will AARNet allow an Identity Provider institution to use a realm which doesn’t include “.au”.

The RADIUS servers that are configured to handle an institutional realm may be a subset of all RADIUS server specified under the “Servers” section.

Realms

Display realms

Search:

Realm	Server(s)	Action
aarnet.edu.au	Server: aarnet.edu.au-2, Type: IdP and SP, Server: aarnet.edu.au-3, Type: IdP and SP	edit delete

Showing 1 to 1 of 1 entries

← Previous **1** Next →

[Add new realm](#)

Edit Action

aarnet.edu.au (edit)

Realm

Proxy to Servers

Server: aarnet.edu.au-2, Type: IdP and SP
 Server: aarnet.edu.au-3, Type: IdP and SP

Only IdP and IdP/SP server types are allowed

[Apply](#)

Add new realm

Add Realm

Realm

Proxy to Servers

Server: aarnet.edu.au-2, Type: IdP and SP
 Server: aarnet.edu.au-3, Type: IdP and SP

Only IdP and IdP/SP server types are allowed

[Apply](#)

Monitoring Data

Eduroam infrastructure monitoring is a goal of AARNet as NRO. In order to perform monitoring, an institutional test account is required to be provided by institutions.

A test account for specific realms (or a single test account that will work with multiple realms) should take the name “eduroam-test@realm”.

The authentication protocols supported should also be specified. It is recommended that PEAP/MSCHAPV2 be the protocols supported & recommended for use by users, as a challenge-response protocol provides an additional layer of security in case of rogue APs/RADIUS servers.

Monitored Realms

Display realms

Search:

Realm	Type	Action	Parameters
aarnet.edu.au	Institution provides account for the NRO to monitor the realm	edit delete	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Method EAP-PEAP</p> <p>Phase 2 MS-CHAPv2</p> <p>Username eduroam--test</p> <p style="text-align: right;"> edit delete </p> </div>

Showing 1 to 1 of 1 entries

← Previous 1 Next →

[Add monitored realm](#)

Edit Monitoring Action

Monitored realm: aarnet.edu.au (edit)

Realm

Monitoring Method

[Apply](#)

Edit Monitoring Account Parameters

aarnet.edu.au parameters (edit)

Realm

aarnet.edu.au

EAP Method

EAP-PEAP ▾

EAP2 Method

MS-CHAPv2 ▾

Username

eduroam--test

Password

••••••••

Do not enter Password
Password is not stored currently

Apply

Add Monitored Realm

Add Realm

Realm

Proxy to Servers

Server: aarnet.edu.au-2, Type: IdP and SP ^
Server: aarnet.edu.au-3, Type: IdP and SP ▾

Only IdP and IdP/SP server types are allowed

Apply

Contacts Data

Eduroam AU policy requires that a technical contact which is a personal contact is provided. A group account (e.g. an IT service desk address) may also be provided.

Ideally there are two administrator contacts provided.

Contacts

Display contacts

Search:

Name	Email	Phone	Action
[Redacted]	[Redacted]	[Redacted]	edit delete
[Redacted]	[Redacted]	[Redacted]	edit delete

Showing 1 to 2 of 2 entries

← Previous **1** Next →

[Add new contact](#)

Edit Contact Account Action

[Redacted] (edit)

Name

Email

Phone

[Apply](#)

Add New Contact

Add Contact

Name

Email

Phone

[Apply](#)

XML File Provided to Global Database

XML data provided to the global database is a subset of data entered via the AdminTool.

As this data provides contact information, access to the institutional data file is restricted to the global eduroam database ingest service and AARNet internal servers.

If you wish to have a copy of the XML data for your institution, please submit a request via support@eduroam.edu.au.

Example XML data for AARNet (with contact info removed):

```
<institutions xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="institution.xsd">
  <institution>
    <instid>2b023ffb5a9b4e699352cc76a79df02a</instid>
    <ROid>AU01</ROid>
    <type>IdP+SP</type>
    <stage>1</stage>
    <inst_realm>aarnet.edu.au</inst_realm>
    <inst_name lang="en">AARNet</inst_name>
    <address>
      <street lang="en">Level 7, Tower A, 799 Pacific Highway</street>
      <city lang="en">Chatswood NSW 2067</city>
    </address>
    <inst_type/>
    <contact>
      <name>...</name>
      <email>...</email>
      <phone>...</phone>
      <type>0</type>
      <privacy>0</privacy>
    </contact>
    <contact>
      <name>...</name>
      <email>...</email>
      <phone>...</phone>
      <type>0</type>
      <privacy>0</privacy>
    </contact>
    <info_URL lang="en">http://www.eduroam.edu.au/</info_URL>
    <policy_URL
lang="en">http://www.eduroam.edu.au/eduroam_AU_policy_v4.1.pdf</policy_URL>
    <ts>2020-06-05T01:46:52.597085+00:00</ts>
    <location>
      <locationid>bd82583ba0f64863ba0794aedd90cd5a</locationid>
      <coordinates>151.20172262,-33.88380346</coordinates>
      <stage>1</stage>
      <type>0</type>
      <loc_name lang="en">AARNet Sydney - UTS</loc_name>
      <address>
        <street lang="en">15 Broadway, Ultimo (Level 10, Building 1 UTS)</street>
        <city lang="en">Ultimo NSW 2007</city>
      </address>
      <SSID>eduroam</SSID>
      <enc_level>WPA2/AES</enc_level>
      <AP_no>2</AP_no>
      <tag>IPv6,NAT</tag>
      <availability>0</availability>
    </location>:
    <location>
:
  </location>
</institution>
```

Feedback on this document should be emailed to support@eduroam.edu.au.