# eduroam AU IdP+SP Audit Checklist

The following is the on-boarding Final Audit Checklist for IdP+SP institutions.

This page will be printed and tables stored as a csv with a column created to record the result of the audit.

For ad-hoc audits, an agreed subset of this audit checklist will be applied.

## Common Audit Items

The following items are relevant for both IdPs and SPs.

### Institution Information

Check institutional information in the eduroam AU AdminTool:

|  |  |
| --- | --- |
| Institution Name | The formal, full name of institution (including “The” if it’s in the formal name). |
| Institution Description | Brief description of the institution and the institution’s business case for participating in eduroam in the intended role (IdP+SP, SP-Only, IdP-Only). |
| Institution Address | Number & Street, City, State, Postcode |
| Institution Primary DN | Institutional registered primary domain name used for generation of the RADIUS Operator-Name attribute, and as the institutional identifier in usage reports, monitoring etc. |
| AARNet customer status | Confirm AARNet customer status and customer identifier if relevant |
| eduroam role | Role for eduroam participation (AARNet will have confirmed that the institution is eligible to participate in the role). |
| Institution homepage URL | Institution’s homepage URL |
| Institution network Access Acceptable Use Policy URL | Confirm the AUP link is valid, with public accessibility, and review the AUP for reasonable “R&E network equivalence”. |
| Institution Privacy Policy URL | Confirm the link is valid, with public accessibility, and review the Privacy Policy |
| Institution eduroam webpage URL | Confirm eduroam webpage. See detailed webpage audit items below. |
| User Security Awareness | Confirm resources available for institutional end-user cyber security training & awareness |

The AdminTool provides a list of participants, including the institution’s formal name, the primary DN, the eduroam role, and links to the institution’s AUP and eduroam webpage.

The institutional eduroam webpage will provide detailed information that might be required by users.

### Institutional eduroam Contacts

For each eduroam contact for the institution:

|  |  |
| --- | --- |
| Contact name | Full name of contact |
| Contact email address | Contact’s institutional email address |
| Contact phone number | Contact’s institutional phone number (mobile is preferable) |
| “Personal” or “Group” | Contact type flag. |
| “Public” or “Private” | Contact exposure flag, determines whether the contact name is published and provided in the XML file for population in the global database |
| “Institutional” or “Campus” | Contact scope flag, if the contact is going to be designated for a particular location |
| “Primary” or “Secondary” | Contact priority flag, if there is more than one contact provided for the institution or campus |

A primary and secondary technical contact must be provided at least for an institution. The primary technical contact should be a personal mail address.

Contact scope “Campus” means the contact will be copied (Cc:) on correspondence regarding a particular campus, the “To:” addressees being the institutional eduroam contact(s).

### Radius Servers

#### Confirm Operability in Role

Using rad\_eap\_test and TMS, ensure that the RADIUS servers are operable in the role the institution intends.

Check international access using CAT also.

#### Deployment

|  |  |
| --- | --- |
| Deployment type | Single, Fail-over, Load-balanced |
| Number of SP RADIUS Servers | >=0 |
| Number of IdP RADIUS Servers | >=0 |

For each RADIUS Server:

|  |  |
| --- | --- |
| Role | Confirm correct operation in required role(s) (IdP+SP, IdP, SP) |
| Accounting | Confirm that RADIUS Accounting requests are not proxied to the NRS |
| Implementation Vendor and Type | E.g. FreeRADIUS, Radiator, CISCO ISE, Microsoft NPS |
| Address support | IPv4-only, IPv4+6 |
| IP Address (IPv4) | Confirm correct IP address is recorded in AdminTool |
| RADIUS Secret | Confirm correct RADIUS secret is recorded in Ansible system |
| RADIUS Protocol supported | RADIUS over UDP |
| Domain name (if registered) | Confirm domain name is noted in config and AdminTool |
| Label (‘friendly name’) | Confirm auto-populated in RADIUS config as <institutional domain name>-n, where n increments from 1 |
| Auth Port | 1812 is default for UDP |
| Acct Port | Leave blank if accounting terminated (recommended) |
| Status Server | Yes/No |
| Attributes Filtered | Minimal attribute list supported? |
| Invalid usernames filtered |  |
| Blacklisted realms |  |
| Chargeable-User-Identity | Yes if CUI released |
| Operator-Name | Yes if ON released |
| Calling-Station-Id | MAC address of user device |
| Framed-MTU |  |
| Monitored | Yes / No |
| Trust configured for TMS | Yes / No if config for NRO Test & Monitoring Server in each RADIUS Server |

#### NRS Configuration

Confirm that NRS client configuration in RADIUS server is correct

#### RADIUS Server Logging

Request a sample of logs captured from the institutional RADIUS server

|  |  |
| --- | --- |
| Awareness of accountability requirement | Ensure logging requirements are understood |
| Required info logged | Confirm required information captured from RADIUS Servers |
| Log retention period | Ensure intent is to retain logs for 3 months |
| Log access authorisation | Ensure logs are protected from unauthorised access |

### eduroam Webpage

#### General

|  |  |
| --- | --- |
| eduroam webpage URL | As above under institutional |
| eduroam Service Description with link to NRO (AARNet) national eduroam website | As per template |
| Institutional compliance with Global and National eduroam Standards with links | As per template |
| Role of institution in eduroam (IdP or SP) | Correct role described |
| For IdP, institutional compliance with AARNet access agreement | For customers, mention of the institution’s requirement to comply with the AARNet Access Agreement |

#### User Responsibilities

|  |  |
| --- | --- |
| Requirement for users to comply with home institution network access AUP | As per template |
| Link to institutional network access AUP | Link to AUP (as under Institutional) |

#### Privacy and User Activity Logging

|  |  |
| --- | --- |
| Link to institutional Privacy Policy | Valid link institutional Privacy Policy |
| Advice to users regarding logging of activity, retention, usage of and access to logs | As per template, information on logging and authorised access to logs. |

#### End-user Support

|  |  |
| --- | --- |
| Advice regarding end-user support | As per template, invitation to seek support with hints on when to seek support from visited vs home institution. |
| Accessing institutional support | Email list and/or phone number |

### Institutional eduroam Support

|  |  |
| --- | --- |
| Support staff training | Confirm institutional staff have had basic training in eduroam |
| Support role | Confirm institution understands their support role, and escalation process to AARNet if required |
| Troubleshooting Tools | Ensure institution is able to use basic troubleshooting tools |

### Access to Usage Metrics

Ensure institution has access to their institutional usage metrics

### Access to & Updating of Institutional Information in AdminTool

Ensure institution has access to and updated its information

SAML IdP

VHO Account

## IdP-Specific Audit Items

The following audit items are relevant for institutions operating as an IdP participant.

### eduroam Realms

For **each local realm** handled by the institution

|  |  |
| --- | --- |
| Realm | Realm string |
| Country-code top level domain name | Confirm country-code (.au) TLDN part of the realm, or understand reasoning why not and request for registration as an exception. |
| Test Account | Username and Password |
| Description | Purpose of realm e.g. for a particular user community |

### User Authentication

For each identity management system used for the institution’s eduroam users:

|  |  |
| --- | --- |
| Identity Management Process | Is institutional Identity Management documentation is available on request |
| Identity Store vendor & name | E.g. Microsoft Active Directory |
| Realms supported | List of realms supported for local authentication using this user authentication mechanism |
| Local Authentication | Is confirmation of authentication configuration provided for users configuring on campus? |
| Authentication Type | TLS or tunnelled EAP (TTLS or PEAP) |
| Inner Authentication Method | (for tunnelled EAP) MSCHAPv2 or PAP |

If TLS, authentication certificate (PEM format) available for home server. If tunnelled protocol, home RADIUS server certificate and CA certificate available.

### Use of Configuration Assistant Tool

|  |  |
| --- | --- |
| Intent to use eduroam CAT | Does the institution intend to use the eduroam CAT? |
| Other configuration authentication automation | If not using CAT, is there an alternate automated device configuration system in use? |
| Certificates configured in CAT | Is the IdP profile for each realm configured with the correct IRS CN and root CA certificate? |
| CAT scripts tested | Have CAT scripts been tested, and for which platforms. |
| Local download of scripts | Are CAT scripts downloaded to a local server |

### eduroam Website IdP Information

|  |  |
| --- | --- |
| eduroam as a remote authentication service | Does the website clearly state the institution’s role as an IdP? |
| eduroam user-name | For each realm, is there clear information on the target user population and example institutional\_username@realm ? |
| authentication method | For each realm, what is the authentication method? Check if PEAP/MSCHAPv2 is supported. If TTLS/PAP, is there warning regarding risks? |
| Links to device configuration (CAT or other) scripts | Are valid links provided, with good description, to the CAT or scripts downloaded from the CAT? |

### eduroam for local users

For the institution’s own users

|  |  |
| --- | --- |
| Is eduroam access the single SSID? | Does the institution use the “eduroam” SSID for local network access for local users? Is it the only SSID? |
| Institution’s use of eduroam for local network access, VLAN segregated | Are local users able to access corporate resources via the eduroam network, and is it segregated from visitors using VLANs |

### RADIUS & Authentication Server Logging

Request a sample of logs captured from the institutional authentication server corresponding to a test authentication.

|  |  |
| --- | --- |
| Required info logged | Confirm required information captured from RADIUS Servers |
| Authentication system logging | Ensure that information is logged as required to enable traceability |

## SP-Specific Audit Items

The following audit items are relevant for institutions operating as an SP participant.

### Wireless Infrastructure

|  |  |
| --- | --- |
| Vendor & Model of Wireless | What is the predominant vendor and model of wireless infrastructure? |
| Standalone APs or WLC? | Does the institution use standalone access points or have a wireless LAN controller |
| Wireless Encryption | MUST be confirmed as WPA2-Enterprise i.e. AES |
| SSID publicly broadcast | “eduroam” (or “eduroam-name” if a special SSID for confirming configuration of user devices for eduroam) |
| Wireless Coverage Map URL | URL for wireless coverage information, including maps |

Assume that wireless infrastructure is consistent across campuses.

### Campus / Location Information

For **each of the institution’s campuses** where eduroam is available, the following information is checked:

|  |  |
| --- | --- |
| Number of APs | Number of access points (gives scale of institutional wireless service) |
| Estimate number of users & identities | Estimate of number of users and identities those users may have enabling eduroam access |
| Campus Informational URL | Any particular website for the campus |
| Campus AUP URL | Any particular AUP for the campus |
| Contacts | *Must be one of the institutional contacts in the eduroam Contact Information table.* |
| Campus name | Formal name of the campus (including “The” if relevant). |
| Location | Confirm Latitude, Longitude |
| Address | Confirm Number & Street, City, State, Postcode |

It’s assumed that SSID, network services are consistent across all campuses.

Campus contact means the contact will be used as the technical contact for a particular campus.

### RADIUS & Network Infrastructure Logging

Request a sample of logs captured from the institutional DHCP server

|  |  |
| --- | --- |
| Required info logged | Confirm required SP information captured from RADIUS Servers |
| NAT/DHCP logging as required to enable traceability | Confirm that DHCP logs enable tracking of allocated IP address to device MAC address |

### Network Service to eduroam users

An important aim of eduroam is to provide visitors with unimpeded access to the Internet, not least because this maximises the probability of a visitor’s applications working as expected.

For auditing, some form of intra-institutional check needs to be done using a laptop connected to “eduroam” with appropriate scripts to confirm the following network characteristics.

#### Protocols/Ports

|  |  |
| --- | --- |
| IPv6 Tunnel Broker Service | IP protocol 41 |
| PPTP | IP protocol 47 (GRE) and TCP/1723 |
| ESP | IP protocol 50 |
| AH | IP protocol 51 |
| ISAKMP and IKE | UDP/500 |
| OpenVPN | UDP/1194 and TCP/1194 |
| IPv6 Tunnel Broker NAT traversal | UDP/3653 and TCP/3653 |
| IPSec NAT traversal | UDP/4500 |
| AFS | UDP/7000 through UDP/7007 inclusive |
| Cisco IPSec NAT traversal | UDP/10000 and TCP/10000 |
| Passive (S)FTP | TCP/21 |
| SSH | TCP/22 |
| HTTP | TCP/80 |
| POP | TCP/110 |
| NTP | UDP/123 |
| IMAP4 | TCP/143 |
| IMAP3 | TCP/220 |
| LDAP | TCP/389 |
| IMSP | TCP/406 |
| HTTPS | TCP/443 |
| SMTPS | TCP/465 |
| Message submission | TCP/587 |
| LDAPS | TCP/636 |
| IMAPS | TCP/993 |
| POP3S | TCP/995 |
| Citrix | TCP/1494 |
| SQUID Proxy | TCP/3128 |
| RDP | TCP/3389 |
| VNC | TCP/5900 |
| HTTP Proxy | TCP/8080 |

#### Network Addressing

|  |  |
| --- | --- |
| Addressing IPv4 or IPv4+6 |  |
| User allocated address via NAT |  |

#### Network Presentation

|  |  |
| --- | --- |
| Segregation of eduroam users via VLANs |  |

#### Application Proxies

|  |  |
| --- | --- |
| Outbound HTTP/HTTPS connections via a proxy |  |
| Proxy implemented as a transparent proxy |  |
| Proxy discovered via DHCP/DNS entry |  |

#### Rate Limiting

|  |  |
| --- | --- |
| Rate limiting of inbound bandwidth for eduroam |  |

#### Wired eduroam

|  |  |
| --- | --- |
| Wired eduroam provided also |  |

### eduroam Website

Information for Visitors (Service Provider Information):

|  |  |
| --- | --- |
| SSID for eduroam | “eduroam” or “eduroam-string” |
| Wireless Encryption | WPA2-Enterprise (8021X/AES) |
| eduroam coverage | Description of campuses where eduroam is provided |
| Link to eduroam coverage map |  |