# Implementing eduroam Roadmap - Part 4

***Last updated: 12/04/2022***

**On this page sections (16),17 - 23:**

17. RADIUS server log keeping and interpretation of logs
18. Monitoring your own service
19. Setting up user devices - 'onboarding users'
20. Q.A. test of your eduroam implementation
21. Promote eduroam at your organisation - your eduroam web site
22. Keep your configuration details data on the eduroam Support server up to date
23. Planning Ahead and Developing your eduroam Implementation

**See Part 1 for sections 1 - 7:** [1]

1. Concepts and terminology
2. Deciding your service type and planning your eduroam implementation
3. Choose RADIUS server platform and plan network connectivity for ORPS
4. Joining eduroam(UK) and selecting your realm
5. The eduroam Support Server website; input organisation/site details, realm name, test account
6. Install your RADIUS Server (ORPS)
7. Acquire server certificate for ORPS/NAS

**See Part 2 for sections 8 - 10:** [2]

8. Firewall configuration to permit RADIUS servers to work with NRPS
9. Add your ORPS to the eduroam(UK) RADIUS Infrastructure via support website and acquire your shared secrets
10. RADIUS Server Proxying to Support a Visited Service and attributes filtering

**See Part 3 for sections 11 - 16** [3]

11. RADIUS Server configuration to support Home user authentication when roaming and on campus; and Attributes Filtering
12. Wi-Fi service and establishment of a VLAN/network service for eduroam
13. Firewall configuration to support eduroam network service
14. RADIUS server software configuration and interoperation with user database
15. DNS Name Server Configuration
16. Test facilities on eduroam Support Server / Visitor Test / Testing a new ORPS

**Part 4**

### 16.1 eduroam Support Server ORPS/Authentication Tests - contd.

3) Log in to the eduroam Support server, click on the 'Troubleshoot' tab on the menu bar. The tests are displayed in the blue Tests panel.

The available test functions are:

- **ORPS Status Check - ICMP ping status test.** This is to ensure an ORPS is up and running at the participant's site.
- **Remote User Authentication Tests.** To check that one of your users at a remote site can be authenticated by your systems. Click on the relevant [Test] button.

  **EAP-PEAP authentication test** - PEAP is commonly used for 802.1X authentication. This option will work for most RADIUS servers. Some servers, e.g., Radiator, may require peaplabel=1 configuration to interoperate with PEAPv1. In this case the following test should be tried:

  **EAP-PEAP (peaplabel=1) authentication test**

  **EAP-TTLS** has various inner types, choose the appropriate one for your site:

  **EAP-TTLS (inner PAP)**

  **EAP-TTLS (inner MD5)**

  **EAP-TTLS (inner MSCHAPv2)**

  Remember that when testing a user from your own organisation authenticating using your 802.1X network, if the user can be authenticated on your network, then provided that proxying works, the user will be able to successfully authenticate at any compliant visited organisation.

  **(PAP authentication** is no longer supported by Support server - PAP is a clear-text authentication method which was common with web redirect systems (Support server v1 originally included support for PAP for the test user account to test basic RADIUS connectivity).

### 16.2 Visitor Authentication Simulation Test

Purposes:

- Testing visiting user authentication during implementaton of a new Visited service to check correct RADIUS forwarding to NRPS
- Verify correct injection of Operator-Name by invoking the automatic O-N check test on the Support server
- Monitor operational status of your ORPS (forwarding to NRPS function) and operational status of NRPS

You can test vistor authentication without needing to request a set of credentials from Janet or a mentor/buddy organisation. The eduroam Support Server will return Access-Accepts for authentication requests for a test user with a userID of 'your_realm' at the realm

'eduroam.ac.uk'. The password is the same password you registered on eduroam Support for your local test user account. Note: until the new Support server goes into production in Q3 2016, Visited-only member organisations are not by default able to use this test service. If you do not have a realm registered with eduroam(UK) Support you should request enabling of this test by sending an e-mail to JSD.

If you have already set up 802.1X authentication on your network, you can use a network-connected laptop/tablet/smartphone or workstation to test authentication of a visitor. Alternatively you can run authentication tests directly from your ORPS using radeaptest, radpwtst or NTRadPing (for FreeRADIUS, Radiator and IAS/NPS respectively).

Key points:

- use your realm as the actual user identity rather than your test account user name (this is to ensure a unique test user name for each participant - several sites have chosen the same name for their test accounts)
- the following realms are supported: roaming.ja.net, janetroaming.net, eduroam.ac.uk, eduroam.org.uk Use whichever/all preferred or relevant to the purpose of your test (.ac.uk, .net, .org.uk are the most commonly encountered eduroam TLDs in the UK)
- use your test account password for this test (not your eduroam Support server password)
- disable certificate validation as this is not currently supported for this test
- the test supports the Chargeable User Identity (CUI) attribute, so if your ORPS sends Operator-Name and CUI with the value 'nul' in the Access-Request, the Support server will reply with a CUI for that user in the Access-Accept

For example, if your realm is "camford.ac.uk" and you have a test account enabled on the eduroam(UK) Support server (as described previously) with the password "password1", then to do a visitor user test at your site, you would simply use the following credentials when promted by your supplicant:

> camford.ac.uk@eduroam.ac.uk [4]
> password1

The alternative way to perform a visitor test is to run test commands from your ORPS. Using radeaptest [5] with FreeRADIUS (via roaming2) this would be as follows:

> Radeaptest your_realm@eduroam.ac.uk [6] <password> roaming2.ja.net 1812 <shared secret for roaming2>

You can also use the eapol_test tool which can be found in wpa_supplicant. See http://deployingradius.com/scripts/eapol_test/ [7]

The service supports PEAP, EAP-TTLS/PAP and EAP-TTLS/MSCHAPv2. (Basic PAP and the use of the FreeRADIUS radtest tool was discontinued since there is no PAP based authentication in eduroam post-captive portal!)

Participants are permitted to use the visitor authentication simulation test for their own monitoring solutions but **should configure any such solutions to not query this service more often than once every 5 minutes**.

**How to set up an_ [8]eduroam service heartbeat monitor?** See: https://community.jisc.ac.uk/library/network-and-technology-service-docs/configuring-eduroam-heartbeat-your-visitor-network

[8]

### 16.3 eduroam(UK) Monitor of ORPS

The eduroam(UK) Support server runs a Nagios monitoring system service for organisations asserting operational services. There are several components of this monitor:

- ICMP 'are you alive' ping (or TCP 2002 for Cisco ACS CSA sites)
- EAP authentication of test account from a remote site (applicable to operational 'Home' and 'Home & Visited' service sites only and only for 'full service' ORPS)
- A scan of the designated URL of your eduroam service information web page for compliance with specified requirements
- DNS dig check for eduroam NAPTR record

ICMP probes run from the eduroam Support server and from all three NRPS every 5 minutes to check basic connectivity and server status, which is why your firewall must be open for ICMP from the NRPS and Support server as described in section 8, firewall considerations for ORPS. **Cisco ACS sites:** for RADIUS servers that cannot accept ICMP, ie Cisco ACS RADIUS servers running CSA, an alternative solution using telnet on TCP port 2002 has been implemented [9]. If you are running Cisco CSA with CSA, please request this option during your induction session or by submitting a request via JSD.

RADIUS authentication probes using your preferred EAP method (originally this test used PAP) are made to participants' realms from all three NRPSs every 5 minutes using the test accounts. This tests that the participating organisation has an operational remote user authentication service for the realm. Since we can control from which NRPS the access-request is sent from, we can test that your realm accepts such traffic from all three NRPS. However we cannot direct RADIUS traffic to a particular ORPS at your realm. Therefore in cases where an organisation has multiple ORPS, it is essential that you check that the shared secrets are correct.

The authentication method used by the probe test was extended from the original PAP-only method and now supports PEAPv0/MSCHAPv2, PEAPv1/MSCHAPv2, EAP-TTLS/PAP, EAP-TTLS/MD5 and EAP-TTLS/MSCHAPv2. The EAP method that organisations actually use for their users can be selected on the site's eduroam configuration page on the eduroam Support web site.

For technical reasons we do not send out automated notifications of failures, however eduroam site administrators now have access to the Nagios system for their particular site (feature added March 2010). After logging on to the eduroam Support server, under the 'eduroam configuration' menu on the left hand pane, select 'Nagios LG'. This looking glass view gives eduroam admins access to the results of the relevant Nagios monitoring processes for their site/realm. Access to this tool should help participants to see more readily underlying issues.

### 16.4 Testing a new ORPS within eduroam Infrastructure before bringing it into production use

The Support server provides the facility for you to set up peering of a (new) ORPS with the NRPS in a protected/test mode. This allows you to carry out your own tests without a specified ORPS becoming part of the production infrastructure and without it being sent live

production or Nagios test traffic. Nb, the eduroam Support on demand EAP tests are also effectively disabled in this mode.

Setting an ORPS to protected/test mode can be achieved by designatating the ORPS as 'test/development' via the eduroam Support server eduroam configuration/Radius Proxy Server menu. Once an ORPS has been set to protected test-mode, only traffic with 'test' prefixed to your realm name will be sent to your test/development server. This enables you to carry out 'loopback' tests using eg: testuser@test.yourorganisation.ac.uk [10]. Nb. When you set an ORPS as test/dev the test. sub-realm is automatically configured in the eduroam(UK) infrastructure, you do not need to set up the sub-realm on the Support realms page.

CAUTION - there is a danger that auth-loops can be created, so it is essential that the local test user account is valid and that you use credentials accurately. At the end of your test session, you must check your logs to ensure that no auth loop has been initiated.

For full details see: ORPS role designation feature on eduroam(UK) Support Server [11].

**FAQs:**

**Why do I get only "Re-sending Access-Request" when testing authentication via the support server?**

Ensure that your firewall is configured to permit UDP ports 1812, 1813 and 1814. RADIUS does not use TCP!

You should also check that your firewall is not discarding UDP fragments. If it is then the configuration should be changed to allow UDP fragments to pass. [Specifically for ipf firewall users, (to be found on Solaris systems) the config script can be changed to PASS fragments using the keep frag keyword].

Rationale - with certain EAP communications, eg EAP-TLS, the RADIUS packet sizes can get much bigger than the usual MTU of 1500. This means that the RADIUS packets get fragmented in transit. Many firewalls are configured to drop UDP fragments (as security against DoS attacks), however this will, of course, break such RADIUS communications. If your firewall is doing such dropping then it will need to be configured to ALLOW such traffic from NRPS<->ORPS. This will affect more sites as people migrate to full 802.1X implementations and use eg EAP-TLS or other EAP methods which use larger packets.

**I'm trying to test my ORPS, but I get Reply-Message = "Misconfigured client: unknown AC.UK site from janetroaming.net. Rejected by <eduroam UK>." when I run the PAP auth test**

If you have configured your OPRS into the Support server config page correctly, the above error is returned because you have set your ORPS as 'Test/Development'. This is resulting in preventing the NRPS from sending any auth traffic, including test traffic to you realm (only traffic with the 'test.' realm prefix will be sent). Refer to ORPS role designation features on JANET Roaming Support Server [11].

## 17. RADIUS server log keeping and interpretation of logs

It is a mandatory requirement of the eduroam Techncial Specification that participating

organisations keep RADIUS logs of authentication traffic.
https://community.jisc.ac.uk/library/janet-services-documentation/eduroa... [12]

Note: Clarification of Policy and Tech Spec Wording - Visitor Activity Logging [13]

It is strongly recommended that eduroam System Administrators make it routine practice to inpsect their RADIUS logs in order to detect any abnormalities and hidden problems.

**Platform-specific Resources:**

Microsoft NPS

Verify that NPS logging is enabled as per https://technet.microsoft.com/en-us/library/cc731085(v=ws.10).aspx [14]

But Microsoft NPS logging leaves a lot to be desired - so it is recommended that you set up SQL server logging. Microsoft documents how to do this here:
https://docs.microsoft.com/en-us/windows/win32/nps/sql-programmability?redirectedfrom=MSDN [15]

You should set up automatic purging of the database so that it does not grow to an unexpectedly large size and you run out of disk space! (6 months is recommended, but this should comply with your data retention policy).

An alternative option is to define some custom views in the Event Viewer. Kevin Burke blogged about this here: https://www.kevin-burke.co.uk/windows-server-technologies/create-custom-view-nps/ [16]

FreeRADIUS

FreeRADIUS website guide to setting up logging in an eduroam environment [17]

Hint: the default main logfile (radiusd.log), which is configured in the main radiusd.conf file and which logs OK messages etc., is rather basic.

Hint: It is recommended to use linelog module for logging - this will enable you to log any of the attributes present in packets. And if you also call linelog in the inner-tunnel authentication phase, attributes relevant to local authentication of your own users can be logged such as EAP type. Rather than fill up your ORPS with log files you can also push logging off to a remote syslog server. And FR 3 includes more funky NOSQL/Logstash stuff.

**FAQs:**

**Can you clarify the Policy/Tech Spec on vistor logging?**

See - community.jisc.ac.uk/library/janet-services-documentation/clarification-eduroamuk-policy-and-tech-spec-wording-visitor Clarification of Policy and Tech Spec Wording - Visitor Activity Logging [13]

**Using the Test facility on eduroam Support web site for EAP-TTLS with PAP inner authentication results in errors in our FreeRadius log due to use of null value outer user name by the eduroam Test. Why is this and what's the solution?**

The log error is due to the eduroam Support server using an outer user name comprising just the realm name for the Test. This conforms to the correct RFC format for anonymous outer identity, in accordance with RFC 4282:

"Omitting the username part is RECOMMENDED over using a fixed username part, such as "anonymous", since it provides an unambiguous way to determine whether the username is intended to uniquely identify a single user."

The eduroam test used to use anonymous@realm [18], however feedback from several organisations led us to adopt the correct RFC format.

ORPS shouldn't be acting on the outer identity unless you **really** need to - this value is easily set to be whatever value you want and therefore must not be used to authorise. The solution is to add a simple addition to the sql.conf which remove this from logging etc. the inner ID should still be accounted and logged.

**The NRPS are only testing one of our ORPSs using the test account configured on the Support server, why is this?**

Janet has set up a system to monitor the RADIUS request handling status of Home organisations, ie. that an ORPS is operational. This is done using the test user account that participating organisations set up on the eduroam Support server.

In your RADIUS logs you are seeing a single NRPS using the eduroam Support test account to check the service status on just one of your ORPS. The reason for this is that the RADIUS check is being launched from the support site and goes via the NRPS. So a NRPS that can handle the request will only pass the request through to the first working ORPS at your site. This validates that your site is currently able to handle eduroam RADIUS requests but does not check that ALL of your ORPS are alive.

The servers can be checked for network connectivity by PING but the only way to check RADIUS would be to allow a direct Support Server to ORPS RADIUS link. This is deemed unacceptable and would invalidate the eduroam check - as we really need to monitor how the NRPS see the ORPS. Monitoring of the status of the ORPS system (be they load balanced, failover or round-robin constructed) is down to the individual organisations.

## 18. Monitoring your own service

A monitoring system should be set up to ensure that you are aware that your eduroam system is operating satisfactorily and that your OPRS is communicating with the NRPS. Nagios is often used for this purpose (and this is what eduroam uses to monitor the availability of participants' authentication systems).

As indicated above in section 15, participants are permitted to use the eduroam visitor authentication simulation test for their own monitoring solutions, but if you do so you must configure any such solution to only query the visitor authentication simulation test service at

intervals exceeding 5 minutes.

If your RADIUS solution supports server-status (FreeRADIUS and Radiator 4.7), you should employ this method to check that your ORPS can successfully communicate with the NRPS (and that the NRPS are responsive).

How to set up an eduroam service 'heartbeat' >
**https://community.jisc.ac.uk/library/network-and-technology-service-docs...** [8]

## 19. Setting up User's Devices/'Onboarding'

One of the hurdles to be overcome in a successful 802.1X institutional deployment is getting the devices of your users setup to work with eduroam. You may have chosen to utilise a third party 802.1X supplicant or to reply on the built in OS supplicant or you may want to support both and/or a variety of EAP methods. Whichever policy you adopt, you are faced with three challenges:

1. Not all devices, operating systems and supplicants are equal with regard to their 802.1X capability

2. Getting requisite third party supplicants and certificates to devices and installed

3. Getting devices properly set up and optimised, including possibly removing legacy configurations and setup SSIDs

Devices and operating system supplicants that are compatible with eduroam

See the geant wiki table: Devices that are compatible with eduroam [19] To a large extent we are at the mercy of product developers to properly implement 802.1X supplicants for thier products and OSs.

Distribution of third party supplicant software and certificates (where applicable)

Once you have decided on the supplicant of choice and the necessary EAP settings there remain a number of potentially major operations:

- Providing connectivity for setup purposes for devices that have not yet been configured for eduroam. Modern OSs have some intelligence built in and if an unconfigured device attempts to connect to your eduroam Wi-Fi service, it can detect the required EAP settings and the user will be prompted to enter username and password. Then the user may or may not be promtped to not validate the server certificate/accept it! With Mac iOS, the user is informed that the certificate is Not Trusted, but can simply click on 'Trust' to proceed. This gets the user onto eduroam, but it is obviously a highly insecure solution and doesn't encourage the user to subsequently change their settings and get their device correctly configured. So preferrably the unconfigurd device should NOT attempt to connect to eduroam. Instead, if the device is corporately managed, you can pre-configure the device by some means. For users' own devices access to an auto-configuration tool is the preferred option - but this required some form of connectivity. The choices are: a) the user's own mobile 3/4G data service (if such a service is available locally) b) a home/public Wi-Fi service c) a walled-garden onboarding / remediation network service that you provide.

- Distribution of third party supplicant software/server certificate CA certificate (to enable trust). You'll need to distribute the third party supplicant software if you have decided not to rely on built in operating system supplicant. (With the introduction of Windows 7 the imperative to use a more satisfactory supplicant than the built in Microsoft Windows software has been reduced - that is, unless your system cannot support PEAP/MSCHAPv2. If your system cannot support PEAP/MSCHAPv2 and you want to support Windows devices you will require your users to use a third party supplicant that does support your chosen EAP method.) You'll also need to ensure that you users' device can trust the CA of your server certificate. So you face the challenge of distributing these. This challenge is easily addressed for corporately managed devices. For users' own devices you will need a web server accessible from the internet or your walled garden intranet. We've produced a guide as an example of how you could set up an on-boarding walled garden, see: https://jisc365.sharepoint.com/:b:/s/PublicDocumentLinks/EcWcgHyqv09Igd8KszmOfvQBLYGh3m [20]
- Getting the user's device properly set up - auto-configuration tools. Finally you'll need to address configuration of whichever supplicant software you've decided to use - a large proportion of users are either relucatant / not up to the job of correctly configuring the software/thier devices. And to be fair, without some help in for instance CA cert installation with Andorid devices, it is not always straightforward. Expecting users to correctly configure supplicants, whether native or third party, is being somewhat optimistic. In particular it is essential that the setup should include configuration of the client for checking of the ORPS certificate! (Without this check, users are susceptible to man-in-the middle expoits to harvest credentials.) Automating this process serves to help both the end user and IT Services, since the burden of fixing misconfigured machines can be eliminated.

There are a number of tools which make the whole undertaking much more manageable:

- eduroam Configuration Assistance Tool (CAT) [21] - this is the preferred option. CAT is a tool that builds configuration installer programs which can be downloaded and distributed under the control of the participating organisation's eduroam sys admin (e.g. via the eduroam service information web page) or downbloaded directly by individuals. To use the eduroam CAT tool (developed through the Geant eduroam confederation), you need to have a compliant Home service and an invite token. To get a invite token go to your eduroam(UK) Support server main configuration page and click on the eduroam CAT invite button. A token will be sent to the e-mail address you have registered as the primary technical contact on the web site. The token expires after 24 hours, so must be used before then. At present you must use social media credentials to activate the account and not the eduGAIN federated access. For more information see the advisory released in the eduroam Blog https://community.jisc.ac.uk/blogs/eduroam/document/configuration-assistant-tool-cat-now-available [22] (link to be updated) and fully documented at https://community.jisc.ac.uk/library/janet-services-documentation/eduroam-cat-configuration-assistance-tool [23]
- Ruckus Network's Cloudpath Enrollment System / Clouthpath ES (formerly XpressConnect [24] before 2015 acquisition by Ruckus Networks (itself owned by CommScope)) - commercial and therefore incurs a cost, but it does support all suppliants - Windows, MacOS, Ubuntu, SecureW2 (and, at the time, the OpenSEA Xsupplicant). We've put together a detailed case study describing why and how Bristol

University rolled out configuration of Windows native supplicant to its users using Cloudpath XpressConnect: Automated 802.1X set-up for eduroam users at Bristol University using XpressConnect [25].
- Historical note: SU1X Windows 802.1X Configuration Deployment Tool [26] - open source, but for Windows only. A few years back we endorsed this option and put together a full page detailing features, benefits and links to case study and operation guide. SU1X has now been interated into the CAT tool.

**FAQs:**

**How do I configure Windows to work with 802.1X?**

Details of all aspects of setting up the client and using eduroam are included in the User Guide [27]. however the following extract details setup of the client in Windows XP.

- 802.1X supplicant configuration for Windows XP [28]

**Why is it important for the supplicant to be set to check RADIUS server certificate?**

For answers to this and to understand server certificate validataion see Kevin Koster's presentation at NWS38 [29] Nb. The Janet Certificate Service CA chain is now USER Trust - UTN-USERFirst-Hardware - TERENA SSL CA.

**Why am I having a problem using eduroam with MS Vista?**

Windows Vista has a slightly different PEAP authentication to that of WinXP. This difference means that Vista 802.1X authentication will not work with older versions of Cisco ACS, RADIATOR or FreeRADIUS ORPS sotware at Home organisations.

Latest versions of these AAA RADIUS servers have been released which fix this problem:

FreeRADIUS 1.1.4 - tested
RADIATOR 3.16 - tested
Cisco ACS 4.1 - not tested (would like feedback from sites using this)

As this issue is only at the authentication end, visitors with Vista should happily be able to use eduroam at a Visited site if their Home site has upgraded their ORPS.

## 20. Q.A. Test of your eduroam implementation

eduroam is a federated service and as such relies on all participants to offer high quality operational services - the Technical Specification is in place to try to ensure this, but by its federated nature there is a degree of trust that participants will implement it faithfully. There is at present no national accreditation process, so we rely on participating organisations to test their implementations thoroughly themselves. An unreliable or badly configured service reflects badly on the rest of the eduroam world and brings the service into disrepute.

**Your network should not broadcast the eduroam SSID until you have an operational service, ie you can tick off compliance to the requirement of the Technical Specification and the following tests can be passed. You can then say with configence that you have a working service.**

**eduroam(UK) Technical Specification Summary of Requirements Checklist** [30]
- tick box list to enable you to verify compliance of your service [31]

**eduroam(UK) Tech Spec Summary of Recommendations Checklist** [32]- tick box to help you assess your implementaton of recommendations [33]

**ORPS - NRPS Communication Test ICMP check** - the reachability of each ORPS must be verified individually. All ORPS must be reachable by UDP and ICMP/TCP (and so your firewall must be configured accordingly) and must be peered with the NRPS and handle RADIUS traffic correctly to support authentication.

From your access to the eduroam Support server, the Nagios LG program can be viewed or the on-demand ping tests can be run to verify ICMP to each ORPS.

- ICMP Check - PING OK

**Authentication Test** - Authentication check from each NRPS to your realm. From your access to the eduroam Support server, the Nagios LG menu option under your eduroam Configuration can be viewed. This tests authentication via the first available ORPS at your realm. This verifies proper configuration of NRPS 'clients' and realm handling on your ORPS

- EAP Authentication Check - access-accept for NRPS0
- EAP Authentication Check - access-accept for NRPS1
- EAP Authentication Check - access-accept for NRPS2

**Visited Organisation - Visitor Authentication Simulation Test** - to verify that authentication attempts by visitors to your service will be forwarded to the NRPS, the visitor authentication simulation test, as detailed in section 15 should be run where applicable.

- Visitor Authentication Simulation Test - success

**Peering Configuration check (verify ALL shared secrets)** - The basic authentication check above only tests authentication via the first available ORPS at your realm. In cases where there are multiple ORPS, the client peering of each ORPS for each NRPS must be also be checked individually. Similarly the visitor authentication simulation test only checks authentication via one of the NRPS to the 'eduroam.ac.uk' realm. Run utilities such as radcheck to verify shared secrets for all ORPS-NRPS combinations, client and proxy.

- to verify proper configuration of all 3 NRPS 'proxy' settings on your ORPS and in multiple ORPS deployments to verify NRPS 'client' configs: radcheck / radpwtest / ntradping tests - ok for each ORPS/NRPS combination

**Correct Realm Handling by ORPS (anti-auth-loop)** - to reduce user authentication/misconfiguration problems and eliminate the danger of your ORPS marking the NRPS as dead due to our ORPS-NRPS authentication loop prevention logic. The test

usernames listed below should be applied to a client on your network and you should check that your ORPS handles realm names correctly and does NOT proxy the authentication attempts up to the NRPS. Such misbehaviour could potentially initiate an 'authentication loop' since logically the NRPS should send the auth-request back to your ORPS and the ORPS would then erroneously send the request back to the NRPS again - causing a never-ending authentication loop as access-requests have no time-to-live limit. This would be a serious situation leading to a loss of service.

To prevent this, the NRPS have anti-authentication loop logic which will drop the misdirected access-requests if your OPRS does forward such usernames. However, since your ORPS will get no reply from the NRPS there is the danger that your ORPS will mark the NRPS as dead - leading to it not forwarding valid access-request packets for a period of time and causing authentication problems. It is therefore important that your ORPS handles username variations correctly.

ORPS username handling tests ('realm' stands for your full realm name eg. 'myorganisationname.ac.uk'):

- testuser@realm [34]@other(egCAauthrealm) - handled locally and NOT forwarded to NRPS
- testuser@UPPERCASErealm [35] - handled locally and NOT forwarded to NRPS
- testuser@validsubrealm.realm [36] - handled locally and NOT forwarded to NRPS
- testuser@realm [34] - handled locally and NOT forwarded to NRPS
- invalidtestuser@realm [37] - rejected locally and NOT forwarded to NRPS

The following section focusses on expands on invalid User-Name (ie those that do not conform to the Network Access Identifier standard).

**Username Handling Conformance Check** - of particular importance in deployments where a single SSID 'eduroam' is implemented at an orgnisation, usernames MUST be in the form user@myorganisationname.ac.uk [38] (.net and .org.uk are also acceptable as is .subrealm.ac.uk etc.) This ensures that users are able to utilise eduroam in a seamless manner when they travel.

The following test usernames should be applied to a client on your network and you should check that your ORPS drops them without authentication against your user database or forwarding to the NRPS:

- testuser (no realm name component) - authentication should be dropped (User-Name MUST contain '@')
- testuser@@anyrealm (contains two '@') - authentication should be dropped (User-Name MUST NOT contain '@@')
- test user@any [39] realm (contains spaces) - authentication should be dropped (User-Name MUST NOT contain ' ')
- testuser@.anyrealm (starts with a dot) - authentication should be dropped (User-Name realm MUST NOT start with '.')

- testuser@anyrealm [40]. (ends with a dot) - authentication should be dropped (User-Name realm MUST NOT end with '.')
- testuser@myorganisationname..ac.uk [41] (contains double dot) - authentication should be dropped (User-Name realm MUST NOT contain double '..')

**eduroam Information Web Site** - you must have an information web site as detailed in the Tech Spec and described in section 18 below promoting eduroam at your organisation.

- eduroam information page on organisation web site - yes

**eduroam Support Server Organisation Congifuration Details Up to Date** - the information you have entered into the web page for your organisation must be up to date, particularly the following:

- Conformance status
- Service level
- 'Test EAP method' should be the EAP method most used by your users
- Individual site details

## 21. Promoting eduroam at your organisation

There are three key elements to promoting eduroam at your organisation:

1. A dedicated 'eduroam service information' page or eduroam section on the Wi-Fi service page on your organisation's web site. This must provide eduroam users with the key information to enable them to use the eduroam service at your site. This is mandatory requirement of the Tech Specification. A content guide is available [42].
2. Advertising the locations at which eduroam is available and raising general awareness of eduroam in your organisation.
3. Providing information to freshers and training if necessary to your own users about the service.

**eduroam service information web page**

It is a mandatory requirement of the Technical Specification that Visited organisations publish information on their web site page for visitors about how to use eduroam at their site. You must update the URL of your eduroam information page on the eduroam Configuration page on the eduroam(UK) Support web site. (This enables this information to be published on our eduroam locations map pages).

Although it is not mandatory for Home only organisations to publish a 'how to use eduroam' web page, it is highly recommended that you publish such a page to provide information for your own users to help them to use the service when they roam to other sites.

For Visited organisations, the Tech Spec requires that their eduroam web page is accessible from both the Internet and from within the organisation in order to allow visitors easy access to information they may wish to refer to.

As a minimum the Visited organisation's web site must include the following:

- The participant’s acceptable use policy (AUP)
- Sufficient information to enable visitors to identify and access the service; the locations where eduroam is available, the eduroam Tier(s), and the SSID(s)
- Information regarding any application or interception proxies that may be deployed and if this is not transparent, how to configure applications to work with the proxy

There is further guidance in the content guide [42].

**Advertising the locations at which eduroam is available and raising general awareness of eduroam**

There is a range of ready-made material published on the eduroam.org web site which you may find useful. This includes a poster, leaflet, information card (business card size), beer mat, sticker, banner. All you need to do is enter the country, NREN and your organisation-specific details in the pdf fields and print on a suitable medium. If you need the Janet logo, please apply for this via Janet service desk.

See: https://www.eduroam.org/eduroam-media-and-resources/ [43]

**Providing information and training if necessary to your own users on the service**

We would suggest that information on how to get started with campus network services includes information about eduroam. You might want to provide an open access captive portal network service for first time users that simply provides information about eduroam, links to your preferred eduroam setup tools and guidance on how to get IT support.

## 22. Keeping your configuration, ORPS, sites location and contact details data on the eduroam Support website up to date

The information you enter on the eduroam(UK) Support site is the source used to populate the www.eduroam.org [44] UK service availability map and the European eduroam database and worldwide map for the benefit of eduroam users. It is therefore important that you keep your organisation's eduroam configuration and eduroam network details up to date.

It is also beneficial to you to regularly check the main config page for your organisation, since issues with the data you supply through the Support portal and your organisation's eduroam service/compliance to tech spec that we detect will be highlighted in the "Detected issues" and "Problem logs" areas on that page. (You should also check the Nagios LG page periodically too). Reminder of how to update details on organisation config page [1].

The most important data entry is done on your main eduroam UK Configuration page, but it is also important to keep the RADIUS proxy servers page and individual sites network information current. After making any changes please hit the relevant [Update] button (located towards the bottom of the pages) for the changes to take effect.

The data requested is detailed below.

eduroam UK configuration page:

- your service type as defined in the Tech Spec
- assertion of the the status of the service you provide
- organisation trading name and legal name details
- test account details
- EAP method to be used in the roaming user monitor test
- requirement in respect of inclusion of troublesome attributes for visitor simlutation test responses
- URL of your eduroam service information web page
- FQDN of your syslog server if you operate one
- requirement in respect of permitting security audits of your RADIUS server by eduroam(UK)/eduroam.OT
- Primary user for receipt of advisories and notices from eduroam(UK)

RADIUS proxy server page:

- RADIUS proxy server FQDN
- authentication port
- accounting port
- priority of ORPS in NRPS servers list (enabling preferred ORPS to be identified)
- function of ORPS - authentication (for Home and Visited) or client (for Visited-only service)
- requirement in respect of Status-Server utilisation
- marking of ORPS as production or test/development server
- operating system
- version
- RADIUS software
- version

Realms page:

- realms

Site Locations page:

- description of location, address, post code and preferrably co-ordinates (*) [particularly if multiple sites at one postcode]
- Number of wireless APs at location
- Wi-Fi ciphers supported (legacy option, since WPA2/AES is the mandatory and only permitted cipher)
- whether wired Ethernet eduroam access is available
- number of eduroam-enabled 802.1X sockets (you will only be able to see the wired socket request if you state you provide sockets)
- is the eduroam visitor network NATed
- does the network traffic on your eduroam visitor network pass through any (transparent) proxy

- are **any** IP port restrictions (inbound/outbound) applied to the network connection
- is IPv6 supported on your eduroam visitor networkork
- optional details for support contacts at the particular location

(*) Use of co-ordinates allows you to get your site much more accurately positioned on the eduroam sites location map and on eduroam Companion. It is therefore recommended that if possible you use co-ordinates (easily determined from web tools such as Streetmap). If you have multiple sites at one post code, to enable the eduroam map to render the locations and for the info you are providing to be of any use in Companion, you **must** use co-ordinates.

If you have a large list of sites which will result in maintaining up to date information becoming an unmanagable administrative burden using the Support portal, you can ask us to update your sites information by sending us a csv file. If you wish to do this, please contact Service Desk to request the required format of the data.

Nb. Only sites stating 'working towards Visited' or 'achieved Visited' compliance will be able to see the fields for the eduroam visitor network (since these are not relevant to Home only organisations). Whilst both 'compliant' and 'no service' organisations can enter values, only organisations asserting that they provide a 'Compliant service' (ie are operational) will have their numbers passed through to eduroam and the eduroam web site.

The information you enter will be made available to the rest of the eduroam community on the main eduroam Support site general page as well as supplied to the eduroam information pages on ja.net and such data may also be in a future RSS/XML feed.

**'Primary user' and additional tech contacts for your organisation** can be updated through the Support server. You can add additional contacts, which you may wish to do if your role with the organisation is changing or you are moving on. How to do this is described in Responsibilities of the eduroam System Administrator [45]. Please let us know through service@ja.net [46] if the sys admin for your organisation changes - we can arrange a fresh joiner's induction call for the new person.

## 23. Planning ahead and developing your eduroam implementation

We plan to add to the documentation available on the Documentation page with features on best practices and ideas to enhance and develop eduroam implementations. We also plan to introduce a 'UK eduroam Technical Development Roadmap' to indicate plans for the progression of the eduroam service and changes to the Technical Specification that will take effect in the UK in the future.

- Create NAPTR records in DNS to Improve Performance of International Roaming for your Users [47]
- Developing your eduroam Implementation [48]

---



**Links**

[1] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-1
[2] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-2
[3] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-3
[4] mailto:camford.ac.uk@eduroam.ac.uk
[5] http://freeradius.org/radiusd/man/radeapclient.html
[6] mailto:your_realm@eduroam.ac.uk
[7] http://deployingradius.com/scripts/eapol_test/
[8] https://community.jisc.ac.uk/library/network-and-technology-service-docs/configuring-eduroam-heartbeat-your-visitor-network
[9] https://thwack.solarwinds.com/thread/11685
[10] mailto:testuser@test.yourorganisation.ac.uk
[11] https://community.jisc.ac.uk/library/janet-services-documentation/orps-role-designation-features-eduroamuk-support-server
[12] https://community.jisc.ac.uk/library/janet-services-documentation/eduroamuk-technical-specification
[13] https://community.jisc.ac.uk/library/janet-services-documentation/clarification-eduroamuk-policy-and-tech-spec-wording-visitor
[14] https://technet.microsoft.com/en-us/library/cc731085(v=ws.10).aspx
[15] https://docs.microsoft.com/en-us/windows/win32/nps/sql-programmability?redirectedfrom=MSDN
[16] https://www.kevin-burke.co.uk/windows-server-technologies/create-custom-view-nps/
[17] http://wiki.freeradius.org/guide/eduroam-logging
[18] mailto:anonymous@realm
[19] https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-CompatibilityMatrix
[20] https://jisc365.sharepoint.com/:b:/s/PublicDocumentLinks/EcWcgHyqv09Igd8KszmOfvQBLYGh3mgv6PmkRca1Vp6
[21] https://cat.eduroam.org/
[22] https://community.jisc.ac.uk/blogs/eduroam/document/configuration-assistant-tool-cat-now-available
[23] https://community.jisc.ac.uk/library/janet-services-documentation/eduroam-cat-configuration-assistance-tool
[24] http://www.cloudpath.net/product_overview.php
[25] https://community.jisc.ac.uk/library/janet-services-documentation/automated-8021x-set-eduroam-users-bristol-university-using-xpressconnect
[26] https://community.jisc.ac.uk/library/janet-services-documentation/guidance-supplicant-configuration
[27] https://community.jisc.ac.uk/library/janet-services-documentation/eduroam-user-guide
[28] https://community.jisc.ac.uk/library/janet-services-documentation/8021x-supplicant-configuration-windows-xp
[29] http://webmedia.company.ja.net/content/presentations/shared/networkshop300310/koster_understandingservercertif
[30] https://jisc365.sharepoint.com/:w:/s/PublicDocumentLinks/ESvAIvWFWflBhlMP-H7nxU0B7UxarO7YdKdmXYwCjAxtLw?e=uO4PCw
[31] https://community.jisc.ac.uk/groups/eduroam/document/eduroamuk-technical-specification-v14-summary-requirements-checklist
[32] https://jisc365.sharepoint.com/:w:/s/PublicDocumentLinks/Efcv7g2JHqFEuTITOqV-mYsBTNfCMlNv4cqBarfRTIpqUg?e=tGloDR
[33] https://community.jisc.ac.uk/groups/eduroam/document/eduroamuk-technical-specification-summary-recommendations-checklist
[34] mailto:testuser@realm
[35] mailto:testuser@UPPERCASErealm
[36] mailto:testuser@validsubrealm.realm
[37] mailto:invalidtestuser@realm
[38] mailto:user@myorganisationname.ac.uk
[39] mailto:user@any
[40] mailto:testuser@anyrealm

[41] mailto:testuser@myorganisationname..ac.uk
[42] https://community.jisc.ac.uk/library/janet-services-documentation/content-eduroam-service-infomation-web-page-guide
[43] https://www.eduroam.org/eduroam-media-and-resources/
[44] http://www.eduroam.org
[45] https://community.jisc.ac.uk/library/janet-services-documentation/what-are-my-responsibilities-eduroam-sys-admin
[46] mailto:service@ja.net
[47] https://community.jisc.ac.uk/library/janet-services-documentation/create-naptr-records-dns-improved-international-roaming
[48] https://community.jisc.ac.uk/library/janet-services-documentation/developing-your-eduroam-implementation