Implementing eduroam Roadmap - Part 1

On this page sections 1 - 8:

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
8. Add your ORPS to the eduroam(UK) RADIUS Infrastructure via support website and acquire your shared secrets

See Part 2 for sections 9 - 14: [1]

8. RADIUS server proxying configuration and attributes filtering
9. Wi-Fi service and establishment of a VLAN/network service for eduroam
10. Firewall configuration to support eduroam network service
11. RADIUS server software configuration and interoperation with user database
12. DNS Name Server Configuration

See Part 3 for sections 15 - 22: [2]

16. Test facilities on eduroam Support Server / Visitor Test / Testing a new ORPS
17. RADIUS server log keeping and interpretation of logs
18. Monitoring your own service
19. Workstation/Laptop Setup/MS Vista issue
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

Part 1

1. Concepts and Terminology

It is recommended that organisations planning to implement eduroam familiarise themselves with the concepts and terminology described in the eduroam deployment guide [3].
Nb. This guide is now showing its age is due for an update.

Resources:

There are useful summaries of concepts and infrastructure components in the European eduroam wiki, which may of help if there any questions unanswered from this web page: general overview [4] and elements of the eduroam infrastructure [5].

Recommended reading: for an introduction to 802.1X, chapters 1 and 2 of 802.1X Implementation at Janet-Connected Organisations [6]

Janet factsheet: IEEE 802.1X [7]

Janet factsheet: EAP Extensible Authentication Protocol [8]

2. Deciding your service type and planning your eduroam implementation

In the UK, Janet-community organisations generally fund and deploy their network systems independently with the result that there is a wide range of ways in which organisations have implemented network services. To enable disparate networks to interoperate for the purpose of user authentication and to provide a reliable and predicable service for the user, Jisc has produced the eduroam(UK) Technical Specification. This defines the service types and the technical standards that must be adhered to by all participating organisations.

Decide the type(s) of service you wish to provide

The first step in planning your eduroam implementation is to decide the type(s) of service you wish to offer for visitors and for your own users and that will best suit your organisation. There are several factors which may influence your decision. Most participants choose to deploy both a Home and a Visited service and Janet encourages this approach. Choose from:

a) **Visited only organisation**: you provide an eduroam connectivity service for visitors to your locations. This may be appropriate if you have no eligible users or are providing the service at a venue which only caters for visitors or you are providing a managed service for a client insitution.

b) **Home only organisation**: your members will be able to benefit from eduroam at other sites. Building a Home service is perhaps technically the most challenging component since the RADIUS server must process authentication requests, acting as an EAP end point and performing user database lookups to your AD/LDAP etc. It is worth bearing in mind that if you deploy a Home-only service and want to provide network connectivity for your users at your own site, you'll need to do this via a non-eduroam network service. This would mean that your users would need to have a Wi-Fi profile for eduroam and another for the local service. Nb. you are not under any obligation to provide any eduroam service for all of your network users - you are at liberty to limit eduroam service to selected users or categories of users).

c) **Home and Visited**: you enable eduroam connectivity for your eduroam-enabled network users for when they roam to other sites and you reciprocate by providing an eduroam connectivity service to support visitors to your site. Your eduroam service can also provide eduroam connectivity for your own users (although you are not under any obligation to provide such connectivity for your own users). If you do authenticate your own users via eduroam on your own site, you may connect them to your eduroam visitors network, but you are not under any obligation to connect them to that. You can connect them to any of your other (non-eduroam) network services - which may be more appropriate since they are at their home site.

The means to do this are described later in this guide.

Whilst you need a good idea of the aim of your eduroam deployment programme and be able to allocate sufficient resources in terms of server hardware, software and time, you don't need to decide every detail of the implementation of your service at the start of the process. Building of a comprehensive eduroam service can be tackled in stages. Indeed a step by step approach is recommended - the various areas are described in this 'roadmap' guide. Technical Support can provide advice and guidance for your project at each stage of implementation.

Recommended viewing - video of James Hooper's presentation overview of the eduroam deployment at Bristol, 'Challenges for wide scale 802.1X deployment [9]'. For slideset, see 'Resources' at bottom of this section. Although showing it's age now, this is a comprehensive overview of eduroam deployment and can be viewed in parallel with the notes below. eduroam CAT is not covered and references to 'Janet' and 'JRS' should now be understood as 'Jisc' and 'eduroam(UK)'.

Consider Wi-Fi and Network Architecture if offering Visited Service

All eduroam services require you to deploy a RADIUS service. Ideally this should be a resilient service and comprise two servers, which may be physical boxes or virtual machines. Selection of the RADIUS server software is covered in the following section.

There is the possibility of outsourcing some elements of your eduroam service, but as ever, particularly regarding Home services, a degree of caution is required since eduroam relates to your core network access authentication system - the management of which is best served through in-house skills.

Consider the technological aspects of the network you wish to offer eduroam over. To provide a reasonably standard experience for users and to try reduce the amount of changes to supplicant and application settings required from site to site, the Tech Spec currently defines a single sets of network parameters based on WPA2 'enterprise' authentication with AES encryption.

[Historical note: In eduroam(UK) documentation you might occasionally come across legacy references to 'JRS Tiers'. The JRS1, JRS2, JRS3 system was withdrawn a number of years ago. Authentication now must be based on 802.1X. Captive portal/web redirection methods are no longer permitted for authentication (these used to be permitted in Tier 1 services). The only authentication method permitted now is 802.1X. Captive portal authentication methods are no longer permitted on 'eduroam' SSID networks, on the grounds of security weaknesses. (It was included in the initial Tech Spec in order to make the service as inclusive as possible). All eduroam tiers used the same national Janet RADIUS infrastructure and users could gain authentication irrespective of the tier of the Home and Visited organisation involved. The differences to the user were simply the wireless cipher options, IPv6 availability and NATing.]

Post-authentication walled-gardens such as where users must click e.g. 'Accept' or load a virus scanner before being admitted to the network are however still permitted. Such systems may be employed for example to assure acceptance of conditions of use or to ensure device patching is up to date or other SoH standards.

Decide EAP methods to support for Home services

If you decide to offer a Home service, you need to decide what EAP authentication mechanism(s) you want to employ. This is an important decision since it will affect how your user's devices must be configured and the driver/supplicant software and certificates needed. The supplicant requirements may also affect how you support installation/configuration, whether an automated client config system can be used and the provision of instructions for your users. The decision on EAP mechanism will also probably involve a review your WLAN setup - if your site has one (nb. you don't need to have a WLAN on your home network site in order to provide an authentication service for your users when they are visiting other organisations and using the remote site guest WLANs).

Your choice of EAP mechanism will be determined by:

i) the RADIUS platform you choose (see section 3 below) (e.g. Microsoft NPS only supports PEAP/MSCHAPv2 and EAP-TLS)

ii) how the credentials on your authentication backend are held/encrypted,

iii) the authentication backend system (AD/LDAP)

iv) the rate of authentications and the number of simlutanteous authenticated users your system will support (some software engines may lack sufficient performance)

v) the client PC/laptop operating systems you wish to support and

vi) the supplicant software you have or plan to install/use on the client devices and may also be influenced by your wireless LAN (if any) setup/vendor support. This may sound complicated, but for smaller organisations the range of options is limited and the decisions are quite easy to make. Seek advice from our tech support team if in doubt.

Advice on selecting EAP methods: Geant eduroam wiki [10]

Consider how users devices are to be configured to work with the service

The method of deploying configuration of the supplicants on devices should be given some thought. Whilst it is possible to just let users do this themselves, this approach will inevitably lead to calls to your helpdesk, user frustration and importantly, insecure device configuration due to incomplete setup of authentication server certificate and server name validation. It is a requirement that you provide device setup instructions but some form of automated setup tool/help system for users is strongly recommended. The section below on User Device Setup gives more details. A number of organisations have implemented open access captive portal setup networks which provide access to their automated setup tools for first time users.

Further Considerations

For participants deciding to offer Visited services (ie most organisations!), a further set of issues must be addressed, particularly the implementation of eduroam VLAN assignment on your wireless access points and wired switches. Also your firewall from the eduroam network/VLAN must permit certain traffic types as detailed in the Firewall Configuration section below.

Without wishing to complicate the process more than necessary, you may wish to consider whether or not you wish to provide guest network services to non-eduroam visitors. These may be visitors from the (very few) UK universities not participating in eduroam, visitors from non-member Further Education colleges, overseas visitors, delegates from outside the community to conferences, alumni and contractors. Some universities only offer eduroam services now! Recommended reading is the Janet guide on provision of network access for guests [11] - the simplest method is through a 'Guests' SSID with a separate non-Janet network feed. You may at the present time however provide guest accounts for use with your eduroam service, but only on strict conditions.

Help is available on all aspects of planning your service from eduroam Technical Support [12]

Resources:

- Challenges for wide scale 802.1X deployment video [9] < highly recommended viewing
- Challenges for wide scale 802.1X deployment slideset [13] < high quality slideset
- Deployment Guide [3]
- Technical Specification [14]
- Comparison of supplicants
- Inter-NREN Roaming Infrastructure & Service Support Cookbook [15] (pdf) (produced and published by GEANT2)

- Consult Technical Support for advice [12]

3. Choose RADIUS server platform and plan network connectivity for ORPS

Choice of Platform

The RADIUS server platform selected will be influenced by the type of credentials employed at your organisation (AD, NDS, LDAP and how certificates are utilised) and consequently the EAP types that you could use. This in turn will affect the choice of supplicant and that may also affect the decision. Other factors will be vendor preference, budget and technical expertise. Most RADIUS platforms however support a wide range of EAP types and authentication back-ends. (Having said that, if considering MS IAS, since this does not at present support EAP-TTLS, the choice falls to EAP-PEAP(MSChapv2) or EAP-TLS (with client certificates).

Options:

- FreeRADIUS website [16]
- Radiator website [17]
- Microsoft IAS (Internet Authentication Service) (Windows Server 2003) website [18]
- Microsoft Network Policy Server (NPS) (Windows Server 2008) website1 [19] website2 [20]
- Cisco ACS (Secure Access Control Server for Windows) website [21]

- Cisco ISE [22]
- Aruba Clearpass [23]
- Juniper Funk Steel-Belted Radius website [24]

Your ORPS may be physical machines or may be VM-based. Experience indicates that Solaris-based VM systems, whilst they function, suffer from a latency issue leading to performance limitations.

Network Architecture

There is no best practice recommendation regarding positioning of your ORPS function in your network architecture. You can connect your ORPS into a DMZ or you can connect it to your internal network to facilitate access to your LDAP/AD. The decision as to where to connect it is up to the organisation and will probably be based on exisiting security policy.

Whatever you choose, the firewall requirements are described in section 8 later in this guide. Note that in the current UDP*/RADIUS-heirarchical model for eduroam, only the NRPS and the Support server will communicate with your ORPS so security can be very tight. Unlike, for instance web servers, which need to be open to the wide Internet, your ORPS operates only in a very narrow RADIUS environment. ([*] Technically you could employ RadSec TLS/TCP, (applicable only to Radiator and FreeRADIUS 3), but again the only communications will be with the NRPS, at present) - Nb. this is not an implementation we are currently advocating).

Your ORPSs must have IP addresses that are reachable and that are resolvable by DNS lookup from the NRPS so if you do wish to employ network address translation, this must be fixed.

Note - 'cloud' based ORPS solutions have not been tested and evaluated by eduroam(UK). Provided that any such solution can meet the Technical Specification they are not probibited, but eduroam(UK) cannot endorse their use.

IPv6 is the recommended protocol for providing NRPS connectivity for your ORPS. However please note that the NRPS do not accept RADIUS requests via 6to4 encapsulation. You should either implement IPv6 throughout the network path to Janet or not enable 6to4 tunnelling on your ORPS.

Separation of RADIUS duties

It is worth considering that the RADIUS proxy server you define as your ORPS does not necessarily need to do any authentication itself. It is perfectly OK to use a relatively simple proxy-only RADIUS server facing eduroam which then forwards any authentication requests received to your NPS server or as needed. One scenario where you might chose to do this is where your chosen RADIUS platform cannot do Operator-Name injection or respond to Status-Server requests or which has poor attribute filtering capabilities and you want to implement these best practice techniques. Another scenario might be that you wish to dedicate an internal RADIUS server to authentication duties and separate the 'proxying' to a second server. FreeRADIUS makes an ideal platform for the proxy-only server in these models.

Resilience

Once your users have experienced eduroam, they will very rapidly come to regard it as an indispensible feature of your network service and your ORPS will become a very important

component. Furthermore, once your ORPS have linked into the RADIUS hierarchy of eduroam(UK) the NRPS will normally expect your organisation to be responsive to RADIUS requests sent to your realm. Whilst there is now logic in place to cope with non-responsive ORPS, it is good neighbourly practice to ensure that your ORPS are up and operational 24/7. It is therefore strongly recommened that participants deploy two fault tolerant servers for resilience. The NRPS will communicate with these in the order in which they were configured, but you will be able to adjust the priority.

Your two ORPS will normally be configured with separate unique shared secrets for communication with the NRPS, but you can opt for the same shared secret to be used on both servers (make you request through Janet Service in the normal way). organisations with Cisco ACS solutions will probably require this.

Help:

- Consult Technical Support for advice [12]

FAQs:

Are there any known issues with certain versions of RADIUS server software?

Yes! We of course make the general recommendation that you keep your RADIUS server software updated to the latest releases. There are particular known issues with versions of the popular choices of RADIUS sofware, including the following:

FreeRADIUS - versions prior to 1.1.4 do not support MS Vista clients due to the change in PEAP handling with Vista compared to XP. 1.1.5 and 1.1.6 had further SSL fixes to improve/fix SSL behaviour and stability in general...as well as more than 30 other bug fixes. If you are sticking to 1.1.x code, 1.1.7 was the final version of the 1.1.x product.

However there is no reason to not upgrade to the 2.0.x or preferably the 2.1.x versions of FreeRADIUS. In 2.0.5, many of the issues in 1.1.x were fixed but 2.1.10 is at the time of writing the preferred release (2.1.11 contains a number of service-affecting bugs).

Radiator - in June 2007 the NRPS had to be upgraded to the current version due to several EAP-TLS broken parts. This was leading to failed authentication attempts from visited sites for users from a participating organisation using EAP- TLS with MS IAS.

The problem, which was traced to the RADIUS exchange not completing, was resolved by upgrading our NRPS Radiator software from v 3.13 to 3.17.1. It is likely that if you are running older versions of Radiator on your ORPS and you get a visitor from a site that utilises EAP-TLS then similar problems will be encountered.

We specifically recommend that if you are still running older versions of Radiator, you should upgrade as soon as possible to the latest version. (Radiator 4.12.1 is the latest version, last modified 30 October 2013).

In addition to the above, a compounding problem was that the ipf firewall software configurations on our NRPS were set to discard UDP fragments. The script was therefore changed to pass fragments using the keep frag keyword. If you employ the ipf filewall on your ORPS, you should check this.

What RADIUS server software are eduroam participants using?

Number of ORPS installations by RADIUS software type:

Number of ORPS installations by RADIUS software type									
	Dec 2006	July 2007	Dec 2007	Apl 2008	July 2008	Apl 2009	Aug 2010	June 2013	June 2014
FreeRADIUS	27	51	59	64	74	74	106	256	308
Microsoft IAS/NPS	12	15	16	21	24	31	47	119	153
Radiator	13	13	13	15	14	16	16	28	34
Cisco Secure ACS	2	3	4	4	10	15	14	23	37
Cisco IOS	0	1	1	1	1	0	1	1	1
Aruba Clearpass	-	-	-	-	-	-	-	-	7
Juniper Steel-Belted	-	-	-	-	-	-	-	-	1
Other	-	-	-	-	-	-	-	-	8
Typo / not stated	14	9	5	6	4	5	0	17	12

4. Select your Realms and Join eduroam(UK)

Selecting your realm

An important parameter to decide is your organisational realm name. This will form the second part of your users' usernames and is effectively the organisation identifier used by eduroam RADIUS servers (at other member organisations and by the national and international eduroam infrastructure) to ensure that authentication requests can be passed back to your organisation when your users roam. The realm name is the '@camford.ac.uk' part of the username (userID@realm [25]).

Your organisation must be entitled to use the requested realm name, ie it must be (or be derived from) a DNS name from the organisation's registered DNS namespace. It is expected that most organisations will request their DNS domain name (eg. 'camford.ac.uk') although it is perfectly acceptable to request a sub-domain name (eg. 'computer-science.camford.ac.uk').

You cannot use internal AD container names (obviously these won't be configured in remote RADIUS servers nor will they be capable of NAPTR record lookups in DNS).

Nb. Your RADIUS server and authentiation platform will need to be able to handle the realm identifier in auth requests. Hint, in Microsoft AD this is usually achieved by using a suitable global UPNs (user principal name) in the AD. This is dcomented in Microsoft Active Directory and NPS technical manuals.

Complete the application form

The next step is to apply to joining the eduroam(UK) federation. This is a very straightforward process - you simply complete the membership application form, which asks for contact and intended eduroam service deployment details. The online form must be endorsed by a senior member of your organisation.

Complete and submit the eduroam application form [26]. Following a validation check and acceptance of your membership to the eduroam(UK) federation a welcome information pack will be e-mailed sent to you. An eduroam(UK) technical consultant will then contact you to arrange a telephone induction call. This call will last 20 - 40 minutes, during which you will be advised of your account credentials for access to the eduroam Support web site, which is the self-service portal for managing your eduroam(UK) participation details including RADIUS proxy servers. The call will take you through the features of the server and you can also use the call to discuss your implmentation plan in detail.

Your eduroam(UK) Support account will enable you to manage your participation details including the creation of sub-realms under the primary realm. Additional primary realms may be requested through the Janet Service Desk. You will also be able to register your organisational RADIUS proxy servers and acquire the requisite shared secrets. You will also be able to carry out tests, view the Nagios monitoring system and access error reports derived from the national proxy server logs. Finally, you will be able to tell us about the service you provide at your site(s), which will then be advertised to the eduroam community. For further details see the section below.

FAQs:

What support services are available?

To underpin the service and to support organisations joining and participating in the service, a comprehensive, fully resourced support structure has been put in place which provides:

- Pre-deployment support ? planning and selection of RADIUS server hardware and software and supplicant systems
- Technical support during implementation
- Post-implementation support on technical issues
- Dedicated eduroam Support server with web front end for eduroam site administrators only
- Participanting organisations RADIUS service monitoring system
- Dedicated e-mailing list for technical and service announcements
- A chargeable consultancy service
- Comprehensive technical and promotional documentation
- eduroam service type and operational status table

- Locations map showing where eduroam is available and the service details at each site

Can individuals join the eduroam from Janet? Is there a way for an individual to obtain an eduroam ID without the user's home institution having to join eduroam?

No. Users must have registered network logon accounts at their home organisations and in order for individuals to use their credentials for authentication at eduroam participating sites, their home organisation has to join eduroam and install a RADIUS server which is peered with the national eduroam proxy servers.

The aim of eduroam is to reduce the amount of administration required both by organisations offering guest access to their networks and for visiting users. This is achieved by users being enabled to use their own usernames and passwords when roaming. Janet has set up the NRPS network and the support service to facilitate this through the eduroam mechanism. There is no facility for users to be issued with independent IDs since this would involve another tier of administration (and defeat the aim of the service).

Do eduroam users have to be registered network logon account users at participating organisations?

Yes. Users must have a network account at their participating home organisation in order for their authentication requests to be validated when they attempt to log on at a visited organisation. They must be registered on their home organisation's AD, LDAP, NetWare etc user database. This is because Janet connected organisations are not permitted to just let anyone onto their guest networks and to access Janet/the Internet via Janet. Furthermore, there is a logging requirement for organisations to record the date and time and user name of eduroam enabled authentications. We have to be able to track down a visiting user if ever there is any security or anti-social usage incident - hence the need to limit the service to registered users.

Can I have a sub-realm for my organisation?

Question a) Does the eduroam spec allow us to configure ORPS to forward user@department.myorganisation.ac.uk [27] RADIUS requests to the department in question's RADIUS server?

Question b) If so, will the NRPS strip off 'department' and forward RADIUS requests to the example-org ORPS?

Answer a) Yes - you can submit any number of sub-realms (such as 'department.myorganisation.ac.uk' as you like. To create a new sub-realm, browse to your organisation in the eduroam Configuration menu on the support web server, and select 'Realms'. Enter the sub-realm name into the Realm name field and press 'Create realm'.

Answer b) No - the NRPS will forward requests bearing these realms to your ORPS unchanged. Because the realm is left unchanged by the NRPS, you can perform additional proxying within your organisation if you wish (for example, to route the request to a departmental RADIUS server). This permits delegation of authentication to other units within your organisation.

Can I request a wild-card realm?

No - however, you are able to define as many "sub-realms" as you require. For example, if your realm is example.ac.uk, you can additionally define bar.example.ac.uk and foo.bar.example.ac.uk.

5. The eduroam(UK) Support Server website; input organisation/site details, realm name, test account

5.1 Welcome to the eduroam(UK) Support Server

The eduroam(UK) Support Server is the primary tool available to you to manage the integration of your eduroam service with the national eduroam(UK) infrastructure. It provides you with the RADIUS shared secrets necessary for peering of your RADIUS server(s) into the eduroam hierarchy. The server also gives you access to a wealth of test and monitoring tools, including on-demand and routine Nagios powered monitoring. The server gives you access to the Service Provider Assurance Tool system and you also have access to extracts from the national proxy logs to assist in troubleshooting. Last but not least, the server enables you to provide details of the eduroam visitor service you provide, which go into the European eduroam database and which are advertised through the European eduroam service locations maps.

The URL of the Support server is support.eduroam.uk. Your credentials for accessing the eduroam(UK) Support Server are supplied during joining/induction. The user name will usually be your organisation's realm name (e.g. 'camford.ac.uk'). Your password is known only to you, but you can reset it if it has been lost or forgotten. There is link to do this on the Home page. The new password will be e-mailed to the Primary user contact address at your organisation; it is to be hoped that this is you(!) If you have newly taken over the role and have not already been added to the Support server you will need to be registered, please contact Janet service desk. We can also arrange a fresh Joiner's induction for you if you wish.

You can add additional tech contacts for your organisation through the Support server. This is useful where a team supports the service or when the lead sys admin or Technical user contact details need to be altered in the event of staff changes. See Responsibilities of the eduroam System Administrator [28] for details of how to do this.

5.2 Assertion of service type and service level

> Log in to the eduroam(UK) Support web site https://support.roaming.ja.net [29] using the credentials supplied during joining/induction. The user name will usually be your organisation's realm name (e.g. 'camford.ac.uk'). Your password is known only to you, but you can reset it if it has been forgotten. The new password will be e-mailed to the primary tech contact address at your organisation; it is to be hoped that this is you(!) If you have newly taken over the role you will need to be registered, please contact Janet service desk.

Once you have logged in, the left hand menu presents the following options:

- General
- **eduroam UK configuration**
- my account
- log out

> Click on **'eduroam UK Configuration'** and select your organisation folder on the left hand

menu panel. Your organisation folder will now expand and the left hand menu will show the following options under your organisation name:

- RADIUS proxy servers
- Realms
- Site Locations
- Test
- Users

(Nagios LG has now been moved to the top level of the lh panel menu)

The right hand panel will now display a series of configuration and information boxes related to your eduroam service. This is one of the key interfaces on the web site.

The first two boxes enable you to assert your service's level of compliance and progress towards full compliance with the eduroam(UK) Technical Specification and your declaration of whether you offer a compliant service yet. Since eduroam is based on a web of trust between participants these are important declarations and in addition determine whether the Nagios monitoring tests are enabled for your ORPS.

Select the relevant 'Compliance level' (Home, Visited, working towards etc.) and 'Service level' (None or Compliant service) from the drop down menus. Click the [Update compliance] or [Update service level] buttons. You must keep these assertions up to date as your eduroam service deployment progresses.

If our Nagios monitoring system detects non-compliance with a mandatory requirement of the Technical Specification, a non-compliance 'Detected issues' box will pop into position as the third box down. Issues triggering this include not having provded the URL of your eduroam service information web site (see later section regardin this).

5.3 Description of Feature Boxes on the Organisation Configuration Page

Normally the third box down will be the 'eduroam(UK) Minor issues' box. Should any issues be detected with your organisation's service an alert will appear here. These will include non-compliance with recommended measures defined in the Tech Spec. These include sending invalid authentication requests to the NRPS, not injecting Operator-Name, no NAPTR entry for RadSec for your realm in DNS. Such omissions are considered as minor issues since not all RADIUS platforms support the measures and therefore these are not mandated. But if you can resolve these issues, please do so.

Also displayed are boxes for:

i) **eduroam CAT invite** - **after** you have asserted that you provide a Home service AND that it is conforms to the Tech Spec, you can request an account on the eduroam (user device) configuration assistant tool which is operated by eduroam Europe. More info [30].

ii) your organisation's **legal name and trading name** (the latter is used for organisation identification on the eduroam participants maps and listings)

iii) **your eduroam test account name** (you will be able to make an entry in this box once you have changed your asserted compliance level from 'none'), test account realm, test account password (which will only ever be seen by eduroam support staff), EAP method to be used

by the eduroam monitor test and option for potentially 'poisonous' attributes to be included in Access-Accepts from the Support Server when you run a Visitor Simulation Test (see later section for more details)

iv) the **URL of your eduroam service information web page** - where you publish key information about your eduroam service provision (AUP, locations where eduroam is available, how to use the service/user guide to configure laptops etc.) See later section for more details and Content for eduroam info web page guide [31]. Please keep this information updated if you make any changes.

v) **Problem log files** - 'Examine log files for this organisation by clicking HERE' the HERE link enables you to view files of extracts from the previous day's NRPS error logs relating to your organisation. Each day the NRPS error events log is parsed for errors and sorted for each member organisation and type of error event. There are three types of log file - The error log files are retained on Support for one month after which they are deleted.

vi) **Syslog server** - coming soon. If your organisation operates a syslog server, we can send syslog data to it in real time. If you would like to benefit from this facility, enter the FQDN of your syslog server in the box and when the feature goes online we'll start sending them the data.

vii) **Security auditing** - you can authorise the eduroam Operations Team, eduroam UK or one of our agents e.g. Jisc CSIRT, to perform security assessments of your ORPS server security or ORPS policies via the eduroam infrastructure.

viii) **Primary user** - your Support Server account name and the e-mail address of the primary user we will send new passwords to should you reset the account and to which we will send out service advisory notices.

5.4 Update 'default location'/enter new site details

> Click on **'Site Locations'** from the eduroam Configuration left hand menu:

- RADIUS proxy servers
- Realms
- **Site Locations**
- Test
- Users

Having completed/updated details of your organisation name and post code in the step above, a default site record will have been created. Under 'Site Locations' on the left hand menu, you will see that 'default site' appears and in the right hand pane a blank 'Create a new site location' panel is displayed.

> Click on 'default site' in the left hand menu. The right hand pane now displays the default details for your main site (limited to postcode and default name, note this Site Location name is 'default location', which will stick out like a sore thumb in the internationally published data unless you update it). Please input the details about the service provided in the various fields. These include; site name and post code, site address (optional), the number of APs, number of RJ45 sockets providing eduroam (eduroam is about 802.1X on wired too), wireless ciphers, NAT if implemented, network traffic proxy if implemented, traffic port filtering if implemented, IPv6 avalability, site support contact details (optional).

If you just provide us with a post code, the Support server will automatically generate co-ordinates which will be used in various location dispaly systems. To ensure that your site location is accurately positioned on the eduroam sites locations map and in the eduroam Companion we recommend you input actual co-ordinates (easily determined from web tools such as Streetmap).

The information provided on this site details page will be used to populate UK members sites data tables on the Community and Jisc web sites and is also used by the eduroam organisation to produce the international and UK sites locations map. The information enables organisations to provide a detailed information about their services to visitors and the rest of the eduroam world. Note, *everything* on this page will be published including the site location description and contact details (hence the site contact details are optional).

> Finish site information update by clicking on the [Update Location] button.

5.5 Details about further sites

> If you have multiple sites at which you provide eduroam, you can create records for these by selecting 'Site Locations' on the left hand menu and then complete the necessary details on the blank 'Create a new site location' panel that appears in the right hand pane. By 'site' we mean a contiguous area of eduroam coverage, so if a campus comprises a number of adjacent buildings in which eduroam service is available, we define this as a singular location. You may provide greater granularity if you wish, but there is a risk that the number of site records will become unmanageable if organisations provide 100s of locations each! Members typically define a handful of sites to upto c.120 for those with faculties/buildings/libraries/halls of residence dispersed throughout city centres.

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.

> Finish site location creation by clicking on the [Create Location] button. If successful, the new site name will appear in the left hand menu under 'Site Locations.'

5.6 Your Realm(s)

Click on **'realms'** from the eduroam Configuration left hand menu under your organisation name:

- RADIUS proxy servers
- **Realms**
- Site Locations
- Test
- Users

> The realm name(s) that you requested on your application to join will be displayed. You can create and delete additional (sub-)realms for your organisation if you require to. Do not delete your top level domain name (if you do, a request must be made to service@ja.net [12] to have this reinstated).

5.7 Create and configure your eduroam Test account

Your eduroam Test User account is an important part of your eduroam implementation and is mandated in the Technical Specification for Home service participants. It is utilised by the eduroam Support Nagios service status monitoring system and can be used by eduroam site administrators to a) verify the function of 802.1X authentication (roaming user test) through the eduroam Support server on-demand Test utility and since the same password is used by the Support server Visitor test b) to verify auth-request forwarding for visitors by your ORPS (visitor authentication simulation test).

Your test account must be created on your local network in the database that authenticatation will be made to from eduroam. This will enable the eduroam Support system to act as a remote user for the test account. It is important that this account is NOT subject to any account locking policies that you may have for general users. (We recommend against account locking measures in general since there are now alternative measures available but it is particularly important that the eduroam test account is not lockable since it is used by the service status Nagios monitor).

To make use of your test account through the eduroam Support server, details of it must first be configured on the server as described below. If you subsequently change the password, whilst on-demand test will work straight away, the Nagios monitor test will only use the new password after the routine configuration refresh which takes place hourly, on the hour.

Configure the Support server with your eduroam Test account details

> Click on **'eduroam Configuration'** and select your organisation folder on the left hand menu pane.

- General
- **eduroam configuration**
- my account
- log out

Your organisation folder will now expand showing the eduroam configuration screen and you can now enter your eduroam Test Account username and password in the 'Test account details' panel on the right hand pane.

>Click on [Update test account] button.

If you have requested multiple organisational-level realms you can select which realm the test account belongs to. You can also select the EAP method that the Nagios service status monitor test uses (PAP is no longer an option) so you should choose the EAP method most generally used by your users.

The left hand menu of the eduroam configuration screen shows the following options under your organisation name:

- RADIUS proxy servers
- Realms
- Site Locations
- **Test**
- Users

To use the Test facility, click on **'Test'** from the eduroam Configuration left hand menu:

Clicking on 'Test' results in the right hand pane displaying the test functions that are available; ping, EAP - see section 15 below. The visitor authentication simulation test can also now be run - see section 12).

To facilitate testing of ORPSs before bringing them into operational use, the eduroam Support website also provides a proxy control and RADIUS traffic routing function. This also supports set up of dedicated role proxying between ORPS and NRPS if required. (This feature can be found under 'RADIUS proxy servers'). Configuration of ORPS in the eduroam Support server is described below in the relevant section 10.

Your organisational firewall must be made ready for the eduroam service at some point. This involves configuring it to permit the passage of required protocols. This can be done now or after your 802.1X system has been set up and authentication tested on your home network.

See: Firewall configuration

6. Install Your RADIUS Server (ORPS)

If you have not already implemented RADIUS on your network, a RADIUS server of your choice must now be deployed. We recommend that software is installed on dedicated hardware or on a virtual platform. Your ORPS must have a unique public-facing IP address and FQDN. The first step is therefore to give your server a DNS name and to create an entry in your DNS zonefile. Next you carry out basic installation of your selected software.

It is strongly recommended that your ORPS is highly fault tolerant and preferrably a resilient dual-ORPS system is put in place. This will require configuration of fail-over or load balancing between the two ORPS. Different systems have differing requirements, but normal practice is for each of your ORPS to have a unique set of shared secrets with the NRPS (the shared secret between roaming0 and ORPS1 will be different from the secret between roaming0 and ORPS2). If your configuration requires both ORPS to have the same shared secret for each NRPS, please open a service request ticket with Janet Service Desk and we will configure the NRPS accordingly. Acquiring shared secrets for ORPS is detailed below in section 10. Nb.

Each of your ORPS must have a unique IP address and FQDN, if you are using NAT for some reason you'll need to have static translation in place.

The reason we strongly recommend you depoly a resilient dual-ORPS system is two-fold, a) for your own service continuity b) but most importantly from an eduroam(UK) viewpoint, to ensure that your realm always has an ORPS available to service incoming authentication requests from the NRPS. If your realm for some reason stops responding to auth-requests and these continue to arrive from your users at remote eduroam sites, a huge amount of NRPS resources will rapidly become tied up and the performance of the NRPS will be drastically reduced. This is because since RADIUS uses UDP, each auth-request results in a UDP socket being held open in the NRPS UDP buffer awaiting a reply. If your realm continues to fail to reply, the load on NRPS resources will increase to the point that effectively service will be denied to other operational eduroam sites - which are handling auth-requests properly. To prevent this situation from affecting the performance of the national service, eduroam will have no option but to suspend service to your ORPS.

Resources:

- Inter-NREN Roaming Infrastructure & Service Support Cookbook [15] - covers various RADIUS platforms (dates from 2008, but still very useful) - 404 error now

FreeRADIUS

- FreeRADIUS official website [16]
- Janet 802.1X Implementation at Janet-Connected Organisations [32] - for an introduction to FreeRADIUS installation and configuration see chapter 4
- FreeRADIUS Demystified Seminar [33] - Alan Buxey's seminal 2012 pre-NWS40 FreeRADIUS Demystified seminar presentation
- FreeRADIUS Best Current Practice Configuration for eduroam [34] - partner material for the FR Demystified seminar
- FreeRADIUS Packet handling; examining the flow [34] - partner material for the FR Demystified seminar
- eduroam.org wiki [35] - FreeRADIUS setup

Radiator

- Radiator official website [17]
- eduroam.org wiki [36] - Radiator setup

Microsoft NPS

- **Microsoft NPS Configuration Guide [37]** - produced by eduroam(UK), step-by-step NPS RADIUS setup guide with screenshots
- Using Windows NPS as RADIUS in eduroam [38] - produced by UUINETT (Norway) so beware of country-specific content, but includes content covering AP config and certificates
- Microsoft IAS website documentation [18]
- Installing Microsoft IAS [39]- TechRepublic article
- MS IAS Operations Guide [40]
- Deployment of IEEE 802.1X for Wired Networks Using Microsoft Windows [41]
- Deploying MS IAS with VLANs [42]

- Microsoft TechNet IAS Troubleshooting [43]

Aruba ClearPass

- Guide to Configuring Aruba WLC and ClearPass [44] - written by UUINETT and likely to have Norway-specific config content!

Cisco ACS / ISE

- See material in the Library [45]

7. Acquire and Install Server Certificate for ORPS/NAS

Depending upon the EAP method you choose to implement, mutual authentication between client and RADIUS server is generally required. The first stage of this is that the client machines need to be able to trust the authenticity of the RADIUS servers and network access servers/APs that they communicate with during the authentication process. The most popular EAP methods require that the authenticating RADIUS server must have a digital certificate. This can be from a legitimate certification authority (CA) or can be self-signed. For information about producing self-signed certificates or for a link to the Jisc Certificate Service (for provision of low cost QuoVadis certificates) see resources section below. Nb The recently defined EAP-PWD method does not require the RADIUS server to have a certificate, however it is not widely supported by suppliants.

eduroam services, being built on 802.1X, are generally implemented using EAP methods that use transport layer security (TLS), such as EAP-TLS, EAP-PEAP and EAP-TTLS - which require the use of a server certificate to authenticate the RADIUS server to the supplicants. In addition EAP-TLS also requires client certificates in order for the clients to be validated by the RADIUS servers. These client certificates may be self-signed, ie. generated by your private CA software.

Self-signed certs/private CA or commercial server certs?

Best practice is to utilise self-signed server certificates or preferrably private CA signed server certificates. These eliminate the potential threat posed by the possibility of a malign agent setting up a RADIUS server masquerading as your ORPS and using a server certificate acquired from the same CA as your legitimate ORPS. The risk is that inadequately set up supplicants, those where server certificate name validation is not enabled, will trust the spoofed ORPS and so will be vulnerable to harvesting of credentials.

You can use a self-signed server certificate, which is one signed with its own private key, but this means that you cannot pre-install trust for it on devices and you will be relying on users to 'click accept' when the certificate alert pops up. This represents poor practice as it conditions users to ignore such alerts - reducing device security. Additionally, having a self-signed cert means that when it expires it you will need to replace it and reconfiguring all client devices - but by having a long expiry date you can balance this effort against the effort of replacing a commercial (e.g. QuoVadis through Jisc's Certificate Service [46]) server certificate on the ORPS.

If you have the necessary expertise to set up a private Certification Authority and issue server certificates you will be able to regate the risk of your ORPS being masqueraded by a credentials harvesting rogue. Use of private CA signed certificates will of course require the CA certificate to be distributed to user's devices and trust of the CA to be pre-configured. But by using CAT, the effort of CA cert distribution and client device reconfiguration can be minimised.

A further benefit of using a private CA is that you will be able to construct a certificate chain without intermediary CA certificates. This results in fewer bytes to be transmitted inside the EAP conversation and hence fewer EAP round-trips and thus faster authentication.

Nevertheless it is recognised that many organisations will lack the time or resources to produce self-signed certificates and to manage the distribution of these to client devices, and whilst this is our best practice recommendation, use of commercial server certificates (e.g. QuoVadis through Jisc's Certificate Service) is a perfectly acceptable!

If you decide not to use self-signed certificates, most RADIUS servers will work without difficulty using certificates from both root certification authorities and intermediate certification authorities such as the Jisc Certificate Service [46] (which supplies QuoVadis certificates at very favorable pricing). If you implement MS Internet Authentication Server however, particular care will be needed in configuring the server because by default it is assumed that the certificate is issued directly from a root certification authority known by the supplicant. This may also apply to NPS.

Server certificate hints

Take care when preparing the CSR for your ORPS(s)!

Certificate type - you need an X.509v3 certificate, ideally Domain-Validated (DV) or Organisation-Validated (OV). SHA-256 is the recommended secure hash algorithm for the signing of the server certificate. The public key should be at least 2048 bits and ideally 3072. Only extended key usage (TLS Web Server Authentication) certificates should be used - not to be confused with Extended Validation (EV) certificates.

Whilst the Common Name (CN) does not have to match the host name of the ORPS in DNS (the CN is just 'a name' and the RADIUS server is not a web server) it is best practice to use a fully qualified domain name as the CN for reasons of maximum compatibility with devices. There should be no spaces in the CN.

The SubjectAlternativeName parameter in the Certificate field should not be empty - the CN and SubjectAlternativeName should have the same value. The CN should not be a wildcard name (e.g. *.camford.ac.uk).

If you deploy multiple ORPS servers, since there is no technical requirement for each server to have a different certificate, it is recommended you use one certificate, imported into all your ORPSs, thereby avoiding issues of support and client configuration/certification. The certificate will have just the one CN component in the Subject field - and that is usually a server name, e.g. eduroam.ORPS1.camford.ac.uk. Note that by using just one CN this will allow you to increase the number of ORPSs in your cluster in the future if required by importing a further copy of the certificate. Note that you can use multiple certificates if you wish, but each certificate will need a unique CN/subjectAltName pair.

The certificate should have the CRL Distribution Point extension to be present. The URL should be valid. In addition, some devices require that the BasicConstraint extension has CA:FALSE set, marking the certificate as being not a CA (the extension should also be marked as critical).

Resources:

- **EAP Server Certificate Considerations** [47] - highly recommended (almost mandatory) reading from the eduroam Europe documentation wiki
- Understanding Server Certificate Validation [48] - video stream of Kevin Koster's presentation to NWS
- Factsheet: Introduction to Server Certificates [49]
- Jisc Certificate Service [50] - lowest cost QuoVadis CA server certificates
- Using certificates issued through the Jisc Certificate Service with Microsoft IAS [51]
- Microsoft technical article: Certificate Requirements when using EAP-TLS or PEAP with EAP-TLS [52]
- TechRepublic paper - Self-sign a RADIUS server for secure PEAP or EAP-TTLS authentication [53]
- Generating self-signed certificates for use with Windows IAS using OpenSSL: Generating Windows IAS PEAP & LDAPS certificates using OpenSSL. [54]
- Generating self-signed certificates using OSC(Radiator)'s CATool? for linux/unix: OSC CATool home page. [55]
- Advisory: Supporting Windows Mobile 8 Certificate Validation [56]
- Advisory: MD5 certificate types deprecated in favour of SHA-1 for RADIUS server [57]

FAQs:

Can I use the Janet Certificate Service to provide certificates for my RADIUS servers?

Yes - the Jisc Certificate Service [58] works fine with the most popular RADIUS servers; FreeRADIUS, Radiator and Cisco ACS and will provide you with server certificates free of charge - suitable for use with EAP-PEAP and EAP-TTLS methods. Previously the service provided 'intermediate CA' certificates issued through TERENA SSL CA and thence chained to Comodo. As of April 2015, the service provides QuoVadis certificates. The use of intermediate CA certificates is considered to be more secure than root CA type. The result of this however is that if you intend to use Microsoft Internet Authentication Service (IAS/NPS) with Janet Certificate Service, a degree of skilful configuration will be required. A technical guidance sheet which details this is available: Using Certificates Issued by the Jisc Server Certificate Service with Microsoft Internet Authentication Service.

The difficulties with MS Internet Authentication Service stem from the fact that it does not

send the full certificate chain during EAP-PEAP negotiation. Consequently, in order to use MS IAS with Janet CS certificates (or any other certificate not issued directly from a certification authority (CA) known by the supplicant), it is essential to:

1. Ensure that you include the correct extensions in the certificate

2. Configure IAS to include the certificate in its list of known certificates.

This issue originally came to light through problems experienced in attempting to use certificates issued by the Janet Certificate Service with the Windows XP supplicant. All certificates issued by the JCS are signed as from an intermediate CA; but any 802.1X supplicant, including the one native to XP, will **not** be able to validate certificate chains derived from intermediate CAs from Microsoft IAS because IAS does not send the full chain in the ServerHello during the TLS handshake in Phase 1 of EAP-PEAP.

So if you intend to use Microsoft IAS, your options are:

1. Use a commercially-supplied certificate that will 'chain directly' to a root CA 'known' by your supplicants.

2. Use a certificate that uses an intermediate CA, but be very careful and thorough in your configuration of IAS. Refer to the technical guide - Using certificates issued by the Jisc Certificate Service with MS IAS [59]. [51]

3. Manage your own private CA.

Nb. Microsoft NPS users must use SHA256 certificates, which the JCS QuoVadis certificates are! "In late 2013, Microsoft announced that SHA1 certificates will not be accepted in Windows after January 2017. At that time, QuoVadis changed its default issuance of SSL to SHA256." https://support.quovadisglobal.com/kb/a429/changes-to-security-indicators-in-the-chromium-browser-affecting-sha1-ssl-certificates.aspx?KBSearchID=34148 [60]

How do I get and install a commercial server certificate for use with MS IAS?

- MS IAS - obtaining and installing a VeriSign WLAN Server Certificate for EAP-PEAP (MSCHAPv2) [61]

Can I use a self-signed certificate for my RADIUS server?

Yes. EAP methods that use TLS, such as EAP-PEAP and EAP-TTLS, require the use of a server certificate to authenticate the RADIUS server to the supplicans.

This certificate may be derived from a local self-signed certificate authority (CA), or purchased from a commercial CA. The advantages and drawbacks of both of these are listed below.

Benefits of a certificate from a self-signed CA:

- No need to purchase a certificate from a commercial vendor.
- Provides a slight security benefit by making it harder for a user to misconfigure their supplicant in an insecure way. (The use of a certificate from a commercial CA combined with a failure by the supplicant to validate the CN of the certificate makes a MITM attack feasible, where the attacker simply acquires a certificate from the same CA).

Benefits of a certificate from a commercial CA:

- No need to distribute the CA's root certificate to each client.

Note: some RADIUS implementations, such as Radiator and FreeRADIUS, provide a certificate from a self-signed CA for testing purposes. Under no circumstanances should this certificate be used in a production environment.

Resources:

- See links in Resources section above

8. Add your ORPS to the eduroam(UK) RADIUS Infrastructure and Add NRPS to your ORPS RADIUS config

You now need to peer your ORPS(s) with the NRPSs so that they can exchange RADIUS communications. This requires the addition of your RADIUS servers as clients in the relevant RADIUS server configurations together with the shared secrets that will establish trust. As state in section 6, your ORPS needs to have a public facing IP address and a fully qualified domain name (an address record in DNS). Your ORPS will be configured in the NRPS clients tables with their IP addresses, but you need to provide us with the FQDNs. This reduces scope for error, facilitates IPv4 and v6 support and enables you to change the IP address in the future without needing to update Support.

Since a there are two ends of the RADIUS conversations there are two operations:

1. Addition of your ORPS to the RADIUS clients configuration of the NRPSs
2. Addition of the NRPS to the RADIUS clients configuration of your ORPSs

8.1 Adding your first ORPS via Support Website and Acquire your Shared Secrets

eduroam(UK) Support is the self-service portal for managing your eduroam(UK) participation details including your ORPS. The account details for accessing Support are provided during the telephone induction call when organisations join the federation. If you forget your password, there is an option for requesting a new one to be sent to the e-mail address registered as the primary eduroam(UK) technical contact for the organisation.

After logging in to Support, select 'eduroam UK Configuration' and your organisation name from the left hand menu. In the left hand menu panel click on '? RADIUS proxy servers'. The 'Create a new RADIUS proxy server' form will appear in the right hand panel.

This form enables you to add your ORPS to the RADIUS clients configuration on the NRPS. Once you click on the 'Create RPS' button at the bottom of the form the details will be added to the ORPS config file on Support and at the next hourly NRPS config update, will be propagated to all three NRPS. Therefore new additions and subsequent ORPS status changes can take up to one hour to take effect! The updated configuration is loaded into the NRPS in the order: Roaming0, Roaming2 then Roaming1, with there being a few minutes between Radiator reloads to ensure continuity of service.

You must enter the following details for your ORPS:

- **Fully qualified domain name:** (The fully qualified domain name of the RADIUS proxy server; do not use the IP address). This field is mandatory. Be sure to update your DNS zonefile to include the server and think about the TTL which will be important if you ever chenge the IP address.
- **Authentication port:** (The port that the RADIUS server is listening on for authentication requests). This field is mandatory.
- **Accounting port:** (The port that the RADIUS server is listening on for accounting requests). This field is mandatory.
- **Priority:** If you have multiple ORPS you may set one of these as 'High priority' - which will result in the NRPS sending authentication requests to this one in preference to the other normal priority ORPS.
- **Function:** The function of the OPRS - authentication only, accounting only, client (no auth or acct packets to be sent to it, but NRPS will accept packets from it - which would be applicable if you provide a Visited-only service), authentication and accounting (the default. These setting enable you to set up the most efficient RADIUS deployment to suit your organisation.
- **Status-Server:** If your ORPS supports it and you wish to use Status-Server, set this to 'Yes'. Status-Server packets very helpfully allow a RADIUS server to determine whether or not another server is alive should no response be received to Access-Request packets. Some RADIUS platforms (FreeRADIUS, Radiator, radsecproxy) support this - if yours does then setting this to 'Yes' will be very beneficial. **Warning!** Do not set this to 'yes' if your RADIUS server does not support Status-Server - doing so will result in your ORPS being marked as dead and it will not be functional. More, see: Status-Server Advisory [62]. **Nb. This function has been temporarily suspended (Sept 2016) and will be reintroduced in Support Server v2 due Q2 2017.**
- **Test/Development:** Relevant to organisations which already have an operational service and wish to peer a new additional OPRS with the national proxies. Servers marked as test/dev will not receive production **or** eduroam test/monitor traffic; only 'anyuser'@test.'your_realm' traffic will be sent to the test/dev ORPS. This enables you to carry out your own testing - which you must initiate through your production ORPS.
- **Operating system name:** (The name of the operating system running on the RADIUS proxy server (for example, "Redhat Enterprise Linux" or "Microsoft Windows")).
- **Operating system version:** (The version of the operating system running on the RADIUS proxy server (for example, "Advanced Server 3" or "2003")).
- **RADIUS software name:** (The name of the RADIUS implementation running on the RADIUS proxy server (for example, "FreeRADIUS" or "Microsoft NPS")).
- **RADIUS software version:** (The version of the RADIUS implementation running on the RADIUS proxy server (for example, "1.1.0" or "2008 R2")).

When complete, click on **[create RPS]**.

You will see the new ORPS listed under 'RADIUS proxy servers' on the left hand menu. By selecting this or any other ORPS you create, the the details will be displayed in the right hand panel enabling you to edit these and view the shared secrets. Remember to hit the 'Update RPS' button if you wish to save any changes.

Your ORPS will be added to the NRPS client configuration on the next scheduled update. This occurs approx 6 minutes past the hour every hour. You must also update your organisation's compliance assertion to ensure that it is 'working towards' or if you already have an operational ORPS, the appropriate operational status. If left at 'None selected' or 'On hold/Deferred' your new ORPS will not be added to the NRPS configuration and the NRPS will ignore any RADIUS requests sent to it from your ORPS.

8.2 Add the NRPSs as RADIUS clients on your ORPS

Underneath the ORPS details panel, the shared secrets with the three NRPS will be displayed. These must be entered into the relevant RADIUS clients configuration files/fields on your ORPS servers. Accuracy is essential when transcribing shared secrets. Ensure that there are no extra characters (white space at beginning or end of the shared secret) and ensure that you are copying and pasting with a correct UTF-8 or ASCII buffer so that characters do not get adjusted when pasting from web browser.

Once the eduroam Support server has refreshed the configurations of the NRPSs, the NRPS will be able to accept and send RADIUS packets from/to your ORPS(s). Note that changes may take up to an hour to be propagated to the eduroam NRPS infrastructure.

There are three NRPSs and any one may try to communicate with your ORPS systems, so you must allow all NRPS to talk to your ORPSs (hint: FreeRADIUS, edit clients and proxy.conf files). You must configure your ORPS for roaming0.ja.net, roaming1.ja.net and roaming2.ja.net to have full auth and accounting passes - 1812/1813 on UDP and be allowed as clients on your ORPS. It is essential that the NRPS are added to you systems using IP addresses and not the Roaming1/2/3 FQDNs! (The NRPSs are IPv6 capable and the addresses are resolvable through DNS. Windows 2012R2 and above NPS users note, NPS is IPv6 aware so if FQDNs are used the ORPS will do a DNS lookup and may select the v6 address and if your site is not fully IPv6 enabled, the ORPS will attempt to tunnel v6 via v4 resulting in communications failure with the NRPS).

Setting up RADIUS forwarding/proxying is described in section 10.

8.3 Adding a Second/any Further ORPS

Additional ORPS can be added to the clients config of the NRPS by following the same steps as described above. It is now quite common practice for organisations to deploy multiple ORPSs, which they may do for resilience or load sharing. You can add as many ORPS as you wish.

Once an ORPS has been added the NRPSs will automatically communicate with it. NRPS send all traffic to the first ORPS in their config list until it stops responding, the NRPS then try the next ORPS in the list. The order of preference is the order which the ORPS were added to the Support server. If you want any particular ORPS to be your primary server, set the 'High priority' option on its config on the Support server, as indicated in section 9.1.

The Support server includes a feature to enable you to connect additional ORPS prior to bringing them into production service. This is achieved through the 'test/dev' setting described above, but full details of this feature can be found in the technical documents section - https://community.jisc.ac.uk/library/janet-services-documentation/orps-role-designation-features-eduroamuk-support-server [63]

Shared secrets for your additional ORPS: Normally every ORPS has a unique set of shared secrets for peering with the three NRPS. This is best practice and the most secure way of employing shared secrets. This remains true even in scenarios in which peered realms contain multiple RADIUS servers. When an organisation registers a second ORPS, by default a further unique set of shared secrets is generated, different from those for the first ORPS. eduroam administrators must be aware that in deployments where the ORPS form fail-over clusters you cannot simply use the original three shared secrets on both ORPSs.

We recognise however that there are particular solutions which use and require a common shared database for all clients and so require the same shared secret for each NRPS to be used by all ORPSs. Where two ORPS are deployed in fail-over systems that use the same set of secrets for each ORPS-NRPS proxy/client config. (ie ?secret0? for roaming0 for both ORPSs, ?secret1? for roaming1 for both ORPSs, ?secret2? for roaming2 for both ORPSs) we can, on request, adjust the details stored on the eduroam Support server, (ie we will duplicate the settings for one of your ORPS). This has had to be done for a number of sites that have chosen a cluster solution that doesn?t allow different keys for remote agents.

If this is required, please choose the ORPS that will be the nominal shared secret seed and which ORPS you want to have adjusted to be the same as that seed and let us know.

Links
[1] https://community.ja.net/library/janet-services-documentation/implementing-eduroam-roadmap-part-2
[2] https://community.ja.net/library/janet-services-documentation/implementing-eduroam-roadmap-part-3
[3] https://community.ja.net/library/janet-services-documentation/eduroam-deployment-guide
[4] https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-Generaloverview
[5] https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-Elementsoftheeduroaminfrastructure
[6] http://community.ja.net/library/advisory-services/ieee-8021x-implementation-janet-connected-organisations
[7] https://community.ja.net/library/advisory-services/ieee-8021x
[8] https://community.ja.net/library/advisory-services/extensible-authentication-protocol
[9] http://webmedia.company.ja.net/content/presentations/shared/networkshop300310/hooper_challengesofwidescalede
[10] https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-SelectingEAPtypes
[11] https://community.ja.net/library/advisory-services/guest-and-public-network-access
[12] mailto:service@ja.net
[13] http://webmedia.company.ja.net/content/documents/shared/networkshop300310/hooper_challengesofwidescaledepl
[14] https://community.ja.net/library/janet-services-documentation/technical-administratorimplementor-information
[15] http://www.eduroam.org/downloads/docs/GN2-08-230-DJ5.1.5.3-eduroamCookbook.pdf

[16] http://www.freeradius.org/
[17] http://www.open.com.au/radiator/index.html
[18] http://technet.microsoft.com/en-us/network/bb643123.aspx
[19] http://technet2.microsoft.com/windowsserver2008/en/library/9af0667e-aa7d-4b1f-a054-7102a85eb2bc1033.mspx?mfr=true
[20] http://technet.microsoft.com/en-us/network/bb629414.aspx
[21] http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html
[22] https://www.cisco.com/c/en_uk/products/security/identity-services-engine/index.html
[23] http://www.arubanetworks.com/products/security/network-access-control/
[24] http://www.juniper.net/products_and_services/aaa_and_802_1x/steel_belted_radius/
[25] mailto:userID@realm
[26] https://community.jisc.ac.uk/library/janet-services-documentation/how-does-organisation-join-service
[27] mailto:user@department.myorganisation.ac.uk
[28] https://community.ja.net/library/janet-services-documentation/what-are-my-responsibilities-eduroam-sys-admin
[29] https://support.roaming.ja.net/
[30] https://community.ja.net/library/janet-services-documentation/eduroam-cat-configuration-assistance-tool
[31] https://community.ja.net/library/janet-services-documentation/content-eduroam-info-web-page-guide
[32] http://www.ja.net/documents/publications/technical-guides/8021x-tg-web.pdf
[33] https://community.jisc.ac.uk/groups/eduroam/document/nws-40-freeradius-demystified
[34] https://community.jisc.ac.uk/groups/eduroam/document/freeradius-best-current-practice-configuration-eduroam
[35] https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-FreeRADIUS
[36] https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-Radiator
[37] https://community.jisc.ac.uk/library/janet-services-documentation/microsoft-nps-configuration-guide
[38] http://services.geant.net/cbp/Knowledge_Base/Wireless/Documents/CBP-13_Using-Windows-NPS-as-RADIUS-in-eduroam_final.pdf
[39] http://articles.techrepublic.com.com/5100-1035-6148579.html
[40] http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5480
[41] http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=7220
[42] http://technet.microsoft.com/en-us/library/cc757645%28v=WS.10%29.aspx
[43] http://technet2.microsoft.com/WindowsServer/en/library/1d497af2-be8a-4e9f-a586-e01bff1862d01033.mspx?mfr=true
[44] https://services.geant.net/sites/cbp/Knowledge_Base/Wireless/Documents/cbp-79_guide_to_configuring_eduroam_using_the_aruba_wireless_controller_and_clearpass.pdf
[45] https://community.jisc.ac.uk/library/janet-services-documentation/cisco-acsise-configuration-eduroam
[46] http://www.ja.net/products-services/janet-connect/janet-certificate-service
[47] https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations
[48] http://webmedia.company.ja.net/content/presentations/shared/networkshop300310/koster_understandingservercertif
[49] https://community.ja.net/library/janet-services-documentation/using-server-certificates-factsheet
[50] http://www.ja.net/services/jcs/service-overview.html
[51] https://community.ja.net/library/janet-services-documentation/using-certificates-issued-janet-certificate-service-ms-ias
[52] http://support.microsoft.com/kb/814394
[53] http://articles.techrepublic.com.com/5100-1035-6148560.html
[54] http://www.cs.bham.ac.uk/~smp/projects/peap/
[55] http://www.open.com.au/catool/index.html
[56] https://community.ja.net/groups/eduroam/article/windows-mobile-8-and-certificate-verification
[57] http://community.ja.net/groups/eduroam/article/use-least-sha-1-radius-server-certificates
[58] http://www.ja.net/jcs
[59] http://community.ja.net/library/janet-services-documentation/using-certificates-issued-janet-certificate-service-ms-ias

[60] https://support.quovadisglobal.com/kb/a429/changes-to-security-indicators-in-the-chromium-browser-affecting-sha1-ssl-certificates.aspx?KBSearchID=34148
[61] http://www.microsoft.com/downloads/details.aspx?familyid=1971D43C-D2D9-408D-BD97-139AFC60996B&displaylang=en
[62] https://community.jisc.ac.uk/groups/eduroam/article/status-server
[63] https://community.jisc.ac.uk/library/janet-services-documentation/orps-role-designation-features-eduroamuk-support-server