FAQs for eduroam System Administrators and Implementation Techs - Part 1

This page lists the most common frequently asked questions about eduroam in the UK. The table of contents summarises the questions asked; please scroll down to the relevant section for the answer. See Part 2 if your question is not addressed here.

Last updated: 12/10/2021

Contents:

- Can alumni have eduroam accounts?
- Do users need to have a network logon account? What about access for the public/non-registered users?
- Can we have an additional top level realm for our organisation?
- Can sub-realms be configured for an organisation?

5) RADIUS server software and configuration

- Do we really need to deploy a RADIUS server, for Viisted services can't we peer our WLCs to the NRPS?
- Links to the various RADIUS server software websites
- How many RADIUS client devices can my ORPS support?
- What RADIUS server software are other eduroam participants using?
- Known issues with particular versions of RADIUS server sofware
- Do you have any example configurations for Radiator?
- Do you have any example configurations for FreeRADIUS?
- What is unlang?
- Where can get up to date binaries for FR2.2 for Centos, which ships with an old version?
- Microsoft IAS implementation advice
- Our AD usernames don't match eduroam username format, how can I strip/modify realm for authentication?
- Cisco ACS implementation advice
- What Attributes should I NOT filter out?
- What procedure do I need to follow for changing the IP address of our ORPS?
- IP Addresses/FQDNs/shared secrets for ORPS - replacing ORPS and moving to a new location
- Shared secrets for ORPS - internal RADIUS servers
- Does Microsoft NPS support RADIUS accounting and how to avoid forwarding accounting packets to NRPS?

6) Server Certificates for ORPS

- Can I use a self-signed certificate for our RADIUS server?
- Use of Jisc Certificate Service
- Can I use the same certificate for more than one ORPS?
- How to configure client workstations to use the JCS TERENA/QuoVadis certificates
- Technical documentation on using MS IAS and Jisc SCS
- Our server certificate is about to expire! What do we do?

7) Integration of RADIUS server with back end user database

- EAP-PEAP authentication against Novell Directory Services
- FreeRADIUS integration with Active Directory
- Radiator integration with Active Directory
- Realm name not in AD - can we get NPS to translate realm?

1) 802.1X and EAP

What is 802.1x and EAP and how do they work?

- IEEE 802.1X [1] - Janet technical sheet on 802.1x outlining its benefits and describing

how it works and listing currently available supplicants together with their main features and applicability.
- Extensible Authentication Protocol (EAP) [2] - Janet technical sheet on EAP, describing how it works, EAP types and implementation considerations.
- Resources about EAP and its support in the current versions of Microsoft Windows [3]

Give me one example of how EAP-TLS is preferrable to PEAP/MSCHAPv2 or EAP-TTLS/PAP

EAP-TLS, which uses certificates, has the advantage that there is not a direct correlation between the certificate and the LDAP/AD password store. Should the user's password be changed in the LDAP/AD, the certificate on their device remains working. If you need to ban a user you would do so by blocking the certificate (eg by using OSCP) rather than by disabling their account. By doing this the user could still read e-mails sent over 3G/4G which could be used to advise them of the password change/network access lock/other reasin why eduroam connection is not working for them. Using MSCHAPv2 notification may also help.

Users do not enter their password credential when logging on with eduroam using EAP-TLS and their password isn't stored in cache on the device, which is a security plus, but of course with EAP-TLS you do need to have and operate a certificate management system.

2) Roadmap for Implementing eduroam

Do you have a step by step process we can follow for implementing eduroam?

Yes, see: https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap [4] ?

Visited service provision - overview of steps required

- Join eduroam(UK)!
- Decide on how your RADIUS server/service host(s) (e.g. a VM host server) will be connected into your network including how the unit will interface with the WLC management network and interface to the internet (some deployments use two network interfaces, others don’t care and just use one for both; next item addresses implications) – give consideration to issues if unit is to be set up in a DMZ. (PS. Some organisations have used cloud-based RADIUS servers/services and for these a VPN link to your WLC management network will be needed.)
- Decide on what RADIUS server software you wish to use - what vendor/command line or GUI/performance/cost you are comfortable with. Acquire the RADIUS software.
- Unless you have opted for an appliance product, set up the server/VM host platform and OS to support the RADIUS software – needs only a basic server specification, but try to opt for maximum fault tolerance or deploy a second server for resilience. (If you have opted for an appliance product, install the hardware.)
- You are planning a Visited-only service with none of your own users authenticating by it so you won’t need a RADIUS server certificate. Feel free to discuss options through the eduroam(UK) support via Jisc helpdesk.
- We address RADIUS server configuration and registration later. At this stage the next step is to connect your RADIUS server host interface 1 to the WLC control network, provisioning IP address for that.

- Connect RADIUS server host interface 2 (assuming two interfaces) to the DMZ/public internet (via firewall if desired), provision IP address.
- Create A record(s) (and AAAA if applicable) in DNS for the RADIUS server(s).
- Set up an eduroam network service for the eduroam-authenticated devices to connect to – comprising IP address pool (private or public), DHCP, DHCP logging, firewall and NATing if applicable (note, only eduroam-authenticated devices can be connected to this network service). Access to a DNS service will also be needed.
- Decide on ports and protocols to be closed with regard to your organisation's security policy - whilst also ensuring compliance with the eduroam Tech Spec which lists the ports/protocols that must NOT be closed. And configure the firewall that will be supporting the eduroam network service. Provision internet connectivity.
- Configure your RADIUS server(s)/service and register your server(s) with eduroam(UK) via the Support portal. This generates the ORPS-NRPS shared secrets you'll need to complete this stage of the RADIUS configuration.
- Configure eduroam SSID on your WLC/APs. Configure your WLC/APs for 802.1X and generate the WLC/AP-ORPS shared secrets to enable completion of the configuration of your RADIUS server to peer with the WLC/APs.)
- Complete the configuration of your RADIUS server(s) to filter out bad usernames/realms and unnecessary RADIUS attributes.
- Test your deployment and verify that it complies with the Technical Specification [5] (checklist available).
- Last but by no means least – create/include on Wi-Fi service information web page the eduroam service information web page for your organisation.

Implementing Govroam alongside eduroam

Of course you would need to join the Govroam federation (free for Visited-only services) and deploy a Govroam SSID and network service for authenticated Govroam user devices... but how could you set up RADIUS efficiently to support both services?

The following presentation shows a high level howto by using the SSID name in the Called-Station-Identity attribute (this may or may not be the case with your APs/WLC) in order to effeiciently implement both services using just one RADIUS service:

https://jisc365.sharepoint.com/:b:/s/PublicDocumentLinks/EYNd3t02k8hGhsEC8K2f338BnKEO5Nrm5b-0aJmdbWgwrw?e=tbytM4 [6]

The alternative is simply to run a second RADIUS service to support Govroam.

3) Networking Issues, Application & Interception Proxies, Firewall Configuration, Ports and Protocols for Visitor services

Can we restrict access to our eduroam Visitor service for devices with obsolete OSs or unpatched devices representing security risks?

Q) We're winding down our support of Windows 7 (or even XP!) and we now deny network access to our own user devices that have not been upgraded/have a long term exception in place. Can we apply the same restrictions to visitors connecting to our eduroam Visitor service? We're concerned that simply denying access will result in many calls to our helpdesk being generated and we don't have the contact details of our regular visitors to even advise them of such a restriction.

A) Member organisations manage and control their own network services and in participating in eduroam make them available for use by eduroam visitors under the terms of the eduroam(UK) Policy and Technical Specification. This arrangement preserves the organisation's right to enforce its own Acceptable Use Policy and Security Policy provided that the Technical Specification is complied with. Therefore, if a Visited organisation wishes to restrict access for devices that are not properly patched or which present an unacceptable security risk, the organisation is perfectly entitled to do so.

Furthermore, there is a clause in the eduroam(UK) Policy stating that organisations 'must ensure that systems that support visiting users are configured, maintained and operated securely, so as not to put the security of other organisations or their users at risk' so there is the expectation that security of user access to eduroam networks is of high importance. Of relevance here are client isolation [7] features that are to be found on high end Wi-Fi APs and switches. With client isolation configured on your APs, rougue/compromised devices will not be able to act as an attack vector to 'good' trusting devices connected to your eduroam service.

If you are going to deploy a restriction/quarantining system, then it is important that it should advise the user about the action taken (*) or that the organisation's **eduroam service information web page** should either provide i) a clear link to the organisation's AUP that states that this restriction applies or ii) a statement that such a the restriction mechanism is in place and what OSs it applies to. The scenario of a user device apparently being authenticated by the home organisation successfully and yet simply not being connected to a network service without knowing the reason can lead to user dissatisfaction - and this should be wherever possible be avoided.

(*) e.g. a captive portal screen is displayed on the suspect device whose access has been restricted when it is connected to a remediation network after successful user authentication.

See query in FAQ part 2 - 1) eduroam Policy Related Issues and Dealing with Virus/Copyright Breach Incidents [8]: Dealing with a virus incident involving an eduroam visitor.

How can we carry out posture assement of devices trying to connect to our eduroam Visitor service?

There are now many older devices in circulation that are still functional and have working software (and so it is tempting to keep in use) but which have old, obsolete and unpatched operating systems such as XP, Windows Vista, older versions of macOS, Mac OS, iOS and Android, that can be vulnerable to exploits. Such devices may still have correctly set up eduroam profiles with valid credentials and may attempt to connect to eduroam services. They represent a significant security risk.

The problem is exacerbated by the fact that there is a widespread lack of user understanding

that a device may be massively out of date, vulnerable and in urgent need of patching despite the device OS not alerting the user the device is highly vulnerable.

How you can actually implement a posture assessment system and restrict access to the Visitor service is not easy to answer, but technically you may do so subject to a few important provisos, see below.

Member organisations manage and control their own network services and in participating in eduroam make them available for use by eduroam visitors under the terms of the eduroam(UK) Policy and Technical Specification. This arrangement preserves the organisation's right to enforce its own Acceptable Use Policy and Security Policy provided that the Technical Specification is complied with. Therefore, if a Visited organisation wishes to restrict access for devices that are not properly patched or which present an unacceptable security risk, the organisation is perfectly entitled to do so.

Furthermore, there is a clause in the eduroam(UK) Policy stating that organisations 'must ensure that systems that support visiting users are configured, maintained and operated securely, so as not to put the security of other organisations or their users at risk' so there is the expectation that security of user access to eduroam networks is of high importance.

Provisos: It is important that **the restriction/quarantining system works with a high level of accuracy** and there should be **a mechanism to advise the user about the action taken** (*) and/or that the organisation's **eduroam service information web page** should provide i) a statement that such a restriction mechanism is in place or ii) a clear link to the organisation's AUP that states that this restriction applies. The scenario of a user device apparently being authenticated by the home organisation successfully and yet simply not being connected to a network service without knowing the reason can lead to user dissatisfaction.

(*) e.g. a captive portal screen is displayed on the suspect device whose access has been restricted when it is connected to a remediation network after successful user.

Detection of legacy devices with a high degree of accuracy:

There are three methods of detecting the 'posture' of a device that we are aware of:

1) DHCP fingerprinting

2) web browser identification

3) embedded software

1. is unreliable at best, 2. requires capturing traffic when visiting a web site (only works if and when a device browses to somewhere - great for captive portals, not so good for 802.1X) and 3. requires the user to install something either permanently or temporarily (difficult to enforce on eduroam visitors). Our understanding is that neither 1 or 2 can identify patch levels or hacked status.

DHCP fingerprinting systems are somewhat of an unknown quantity and systems operate with a closed algorithmic determination process which is likely to be unpublished. So this opaque process may get things wrong in a hard-to-diagnose kind of way.

In conclusion, we would advise caution about restricting access by either the fingerprinting method or agent installation as these could mis-identify a lot of devices, with both false positives and false negatives resulting in users experiencing a poor quality of service.

Is web content filtering permitted on eduroam services?

Filtering of web traffic both URL or content-based, whilst not encouraged, is permitted on eduroam services – provided that TLS/SSL interception is not employed in respect of services for visitors.

Furthermore, an organisation can setup a local VLAN/network segment for its own eduroam users on which the organisation can implement any policy it choses (including web content filtering) and when users are at their home organisation, local users once authenticated, can be connected to this local VLAN (using dynamic VLAN assignment). Visiting eduroam users however must be connected to eduroam-compliant network services (refer to Technical Specification).

Can TLS/SSL interception proxies (for instance as used in content filtering) be deployed?

The Technical Specification v 1.3, whilst advising against such deployment, stated that Visited organisations may in fact install application or 'interception' proxies, provided that the fact that such a sysem is being used is published on the eduroam service information page. Furthermore, if a proxy is not transparent, instructions for the configuration of applications to use the proxy must be published. Version 1.3 of the specification went on simply to note that "interception proxies, often used by intrusion and virus detection systems, may result in the user experiencing unexpected network behaviour."

This policy was formed with the use of proxies such as Squid in mind. Over the past year or so the deployment of TLS/SSL interception proxies has become more popular. Such proxies are employed in some content filtering systems, particularly those filtering HTTPS content (and may also be used in some intrusion and virus detection systems). TLS/SSL interception requires the user to install a CA certificate from the intercepting organisation. This is undesireable for a number of reasons. It requires significant effort by the user. It also results in the proxy breaking the secure path between user and service. It is in effect a man-in-the-middle interception and is contrary to recommended security practice. Several web browsers will flag up the security deficiency to users, who may then discontinue their (legitimate) use of the network. The v1.3 specification advised simply that unexpected network behaviour might be experienced, and noted that significant effort would be required by the user to install certificates from (untrusted) third parties.

There is an interesting article on the pros and cons of HTTPS interception at: https://www.helpnetsecurity.com/2017/03/08/https-interception-dilemma/ [9]

The policy of eduroam(UK) has now evolved in response to the development of TLS/SSL proxies and a new version of the Technical Specification has been released. ***Version 1.4 of the Tech Spec requires that TLS/SSL interception proxies are NOT permitted on eduroam network services that visiting eduroam users are connected to.***

It should be noted that organisations are not obliged to connect their own users when they are

at their Home organisation to the eduroam Visitor network. Rather, local users may be connected to non-eduroam network services suited to local users as required for instance where deemed necessary for a college to implement its policies on Prevent and Safeguarding. So you would been to implement dynamic VLAN assignment such that your own users are connected to the filtered and monitored network that they currently use and visitors are connected to a non proxied/intercepted network service (aka an eduroam VLAN). This eduroam network service needs to comply with the eduroam(UK) Technical Specification.

It should also be noted that content filtering not involving interception proxies IS permitted on eduroam network services for Visitors (providing its use is advertised), although this is not encouraged.

Can users' traffic be monitored and analysed?

Q. We are contemplating data mining of the websites visited by eduroam users (for the purpose of providing analytics on the most visited web pages and repeat visits since such metrics are very useful to our collections staff and such data would prove to be force multipliers for much needed funding bids to demonstrate delivery of resources).

The eduroam T&Cs do not prelude the monitoring and analysis of traffic but clarification is sought on whether we can:

Log our eduroam users' outbound traffic and analyse the traffic for frequently used websites and repeat visits, given that we anonymise the data so that is not personally identifiable and delete the information when no longer needed.

A. eduroam policy does not say anything about a member organisation monitoring of use of the network. However the ability to monitor suggests that a proxy may be utilised somewhere. If so, this needs to be documented to assist Jisc in any debugging that may be required. Such a proxy must also comply with eduroam(UK)'s restrictions on the employment of TLS interception. In addition, the depolyment of monitoring and analysis of traffic on the eduroam service must be advertised on the organisation's eduroam service information web page.

Moreover there are some laws that need to be complied with:

At present, the Data Protection Act 1998 requires organisations to inform users of any processing of personal data, which would include logs of IPaddr/URL etc. The organisation also needs to work out which legal basis applies to the processing (Data Protection Act 1998 section 6), and ensure it meets the relevant requirements of that basis. If the organisation is using the information for internal purposes then one option is "Necessary for the Legitimate Interests of the Data Controller" (art.6f), in which case it needs to ensure that any risk of impact on the individual is minimised *and* that any remaining risk is justified by the benefit to the organisation. There is an introduction to the different legal bases, as they will be from May 2018 under the General Data Protection Regulation, at https://community.jisc.ac.uk/blogs/regulatory-developments/article/gdpr-... [10]. That article also includes a link to the ICO's thoughts on the requirements for consent to be valid under the GDPR, which becomes relevant, because...

Things are going to get more complicated from a date that the European Commission would like to be 25th May 2018. That's the proposed start date for a new ePrivacy Regulation. The current draft of that will prohibit all uses of information relating to the use of electronic

communications networks - both content and metadata - unless:

a) it's necessary for providing the network, or

b) it's necessary for securing the network, or

c) you have the individual user's positive, informed, consent.

So under the current draft, consent is likely to be their only option. The legislation is at a very early stage - the Commission has published their draft, the EU Parliament has decided which committee is going to discuss it, and the Council of Ministers has had one meeting - so there are likely to be changes. There's also the question of how that timetable relates to Brexit, which adds a further layer of uncertainty to what the UK might implement. Advice for designing a system for user monitoring, would include a contingency for a *lot* of change, or indeed having to turn it off, in a year or two's time.

Can private IP addressing with NAT be provided for visiting eduroam users?

We are currently providing visiting users with public IP addressing, however we are fast approaching capacity on the allocated subnet. Can we change the addressing to RFC1918 and NAT (NAT overload) their connections via our routers/firewalls?

Yes, you can implement private networking with NAT for all eduroam users (your own and visitors). You simply have to ensure that the ports and protocols that must NOT be blocked as specified in the Technical Specification at least are open for devices connected to your eduroam network service for visitors.

The following address ranges are used for private networks, as specified in RFC1918:

```
10.0.0.0        -   10.255.255.255  (10/8 prefix)
172.16.0.0      -   172.31.255.255  (172.16/12 prefix)
192.168.0.0     -   192.168.255.255 (192.168/16 prefix)
```

NAT overload is the most commonly implemented form of NAT. There is an excellent article about this at:

http://www.firewall.cx/networking-topics/network-address-translation-nat/233-nat-overload-part-1.html [11]

Is PPTP considered secure and can it work with NAT?

Q. "eduroam network must permit TCP port 1723 and IP protocol 47 in order to support PPTP, but surely PPTP is regarded as an insecure protocol these days?"

A. Almost all protocols that people use are insecure in some way - usually due to the way that a site or system implements it. PPTP is a weaker for of VPN and , like many protocols, there are ways of attacking it - but sites/people still choose to use PPTP for basic VPN usage and that's their choice.

Q. Can PPTP be made to work with NAT?

A. PPTP and NAT can be made to work fine together - after all, PPTP works fine at most

people's homes and it is commonly used to connect to work networks - most people have NAT on their home Internet services. So PPTP and NAT coexistence depends on the firewall being used and whether a site needs to activate some extra helper.... natively it won't work as the PPTP session has source/destination address - the system needs a pass-through or helper to keep track of the session.

We can authenticate and get connected to eduroam ok, but client states "no internet" and we can't access web pages.

We did an OS upgrade on our firewall and although that appeares to have been successful, since then we've been experiencing this problem.

If devices can connect to eduroam then the authentication part of the system, which eduroam deals with, is running OK. The local Wi-Fi service provision on the other hand can be affected by many things. Since your firewall was upgraded recently, the chances are this is where the problem lies. Check sequence:

1) Are connected devices assigned an IP address?

If no IP address is assigned there is a DHCP issue - is the DHCP service provided by the firewall and is it running/configured correctly?

2) Are they assigned a DNS server and can they resolve URLs?

If not there's a DNS resolver issue - how are DNS resolvers made available to clients?

3) If any access to local network resources should be available, does that work?

If local access is OK then there is an internet access problem - firewall permissions for outbound traffic and any NAT config should be checked. Are the requisite ports and protocols correctly enabled?

4) Joining eduroam / Realms / Eligibility

- Can individuals join eduroam?
- Can a person have an eduroam ID without host org joining eduroam?
- Is eduroam available to all members of an organisation?
- Do users need to have a network logon account? What about access for the public/non-registered users?
- Can we have an additional top level realm for our organisation?
- Can sub-realms be configured for an organisation?

Can individuals join eduroam? / Can a person have an eduroam ID without host org joining eduroam?

No. Individuals can only use eduroam as members/associates of an organisation that itself is a member of eduroam(UK) and that acts as an identity provider, i.e. an IdP / Home service participant. The member organisation authenticates the user. eduroam(UK) does not act as an identity provider/authenticator (apart from for Jisc staff members). Even if the organisation with which the individual is associated is part of the Jisc community, the host organisation must be a member of eduroam(UK).

Is eduroam available to all members of an organisation?

To whom the member organisation grants a network access account and to authenticate is a matter for the organisation to decide, provided that the various Janet AUP and Security policies are complied with and that the private network status of Janet is not compromised; this results in the exclusion of general members of the public and alumni who are not currently actively engaged with the organisation/university. Temporary visitors such as conference delegates and people engaged in joint research with the organisation/university may be given network accounts strictly for the duration of their association with the university. This is all covered in the documents under https://community.jisc.ac.uk/library/janet-policies/eligibility-policy-guidance [12]

All members of organisations whose primary business activity is research or education are eligible to be given credentials for eduroam roaming.

Organisations whose primary activity is not research or education, but who are nevertheless eligible to participate in eduroam(UK) (e.g. local authorities, national health service organisations and other public sector bodies - see separate FAQ) as a Home service (IdP) provider, must limit eduroam roaming capability to those members who are engaged in research, education, training or support of these activities.

Can alumni be granted eduroam accounts?

The Janet AUP, Security Policy and the private network status of Janet result in alumni generally being ineligible to be granted network access privileges and hence eduroam enabled accounts. Together with former members of staff, alumni may only be given eduroam credentials if they have an ongoing close association with / are currently actively engaged with the organisation/university / are on site for the purpose of contributing to the organisation's primary business activity (research/education).

The network accounts of students/researchers/staff who have left the organisation and no longer have a close association should be promptly disabled, as least in respect of eduroam and the leavers should be encouraged to delete the eduroam profiles from their devices.

Do users need to have a network logon account?

Yes, users need to be authenticated by their host organisation. Such authentication is for the purpose of providing eduroam network access. Most organisations deploying eduroam make eduroam their primary network. It would be permissible for a user to have an eduroam account that the organisation did not permit local network connectivity for - although we can't think why. A more understandable scenario would be where a small organisation did not provide its own eduroam Wi-Fi service but still acted as an eduroam IdP, for instance an organisation that is hosted by/embedded in a university/NHS trust/local authority.

What about access for the public/non-registered users?

To whom the member organisation grants a network access account and to authenticate is a matter for the organisation to decide. Such users will invariably need to register to be granted a network access account. Organisations may grant temporary accounts for visitors to conferences, events, training courses, contractors etc. provided that the various Janet AUP and Security policies are complied with and that the private network status of Janet is not compromised. Unregistered access for the public is not permitted - see the Janet factsheet on Guest and Public Network Access https://community.jisc.ac.uk/library/janet-policies/guest-and-public-network-access [13]

Can we have an additional top level realm for our organisation?

Yes, provided that your organisation is entitled to use the DNS domain. The technical wording is 'owns or manages by delegation'. We interpret this to include realm names/sub-realms that the organisation owning the DNS domain has given permission for your organisation to use for eduroam. To request an additional top level realm, simple put in a request via the Jisc Service Desk / Jisc online service request form.

Can sub-realms be configured for an organisation?

Yes. This is a self service function that sys admins an perform via the eduroam(UK) Support server portal.

5) RADIUS server configuration

In this section you will find specific information on Radiator, FreeRADIUS and MS Internet Authentication Service / Network Policy Server as well as information relevant to all RADIUS software.

Do we really need to deploy a RADIUS server; is it forbidden to simply peer our WLC to the NRPS (particularly for Visited-only services)?

Yes, pretty much. (This question is also addressed in section 9 on https://community.jisc.ac.uk/library/janet-services-documentation/faqs-eduroam-system-administrators-and-implementation-techs-0 [8])

It would be technically possible to configure WLCs as clients of remote RADIUS servers - you would need to allocate a public IP address for each WLC, create A records in your DNS and configure your firewall to support the addresses and forward to your WLCs. You would also need to set the WLCs as your 'ORPSs' in the eduroam(UK) Support server portal. However, this is strongly deprecated and there are further technical issues to be considered.

The deployment model on which eduroam is based is that of a RADIUS server being peered to the NRPSs with the member organisation's APs/WLCs providing the Wi-Fi service and pointed to the RADIUS server for authentication. The Technical Specification (to underpin the trust fabric of eduroam and to comply with security policies) requires that there is logging of authentication events. It also requires that non-essential VSA attributes, which in many cases essential to internal network operation, are not included in authentication responses to the NRPS/visited ORPSs - so it may be required that your system can support attribute filtering. In addition, some authentication filtering based on realm may be required. For all these reasons, unless your WLC system can support the aforegoing, the deployment of a RADIUS server is the strongly preferred solution.

Having a dedicated RADIUS server allows you to implement the following:

1. Choose a fully functional RADIUS server/service that meets your requirements/vendor supply policy (*)
2. Makes it easier to provision a public facing IP address c/w A record in DNS - one ORPS can support multiple WLCs
3. Put in place authentication filters to ensure that rubbish auth requests containing malformed/bad/nuisance usernames are not sent to the eduroam(UK) servers
4. Put in place RADIUS attribute filters to remove spurious/troublesome attributes that may ‘leak’ out of your own and other member organisation services as required in the eduroam(UK) Technical Specification
5. Comply with the eduroam(UK) Technical Specification RADIUS logging requirements [14]
6. Allow for upgrades/replacement of WLC separately from RADIUS service function

(*) There are several top quality RADIUS server systems available: FreeRADIUS, Aruba ClearPass, Microsoft NPS, Radiator, Cisco ISE etc

Do you have links to the various RADIUS server platform websites?

FreeRadius website [15]

Radiator website [16]

Microsoft IAS (Internet Authentication Service) (Windows Server 2003) website [17]

Microsoft Network Policy Server (NPS) (Windows Server 2008 and Windows Server 2012) website [18]

Cisco ACS (Secure Access Control Server for Windows) website [19]

Juniper Funk Steel-Belted Radius website [20]

How many RADIUS client devices can my ORPS support?

Please note that this answer relates to RADIUS clients (eg NAS devices - such as wireless access points and switches) NOT actual users using the ORPS.

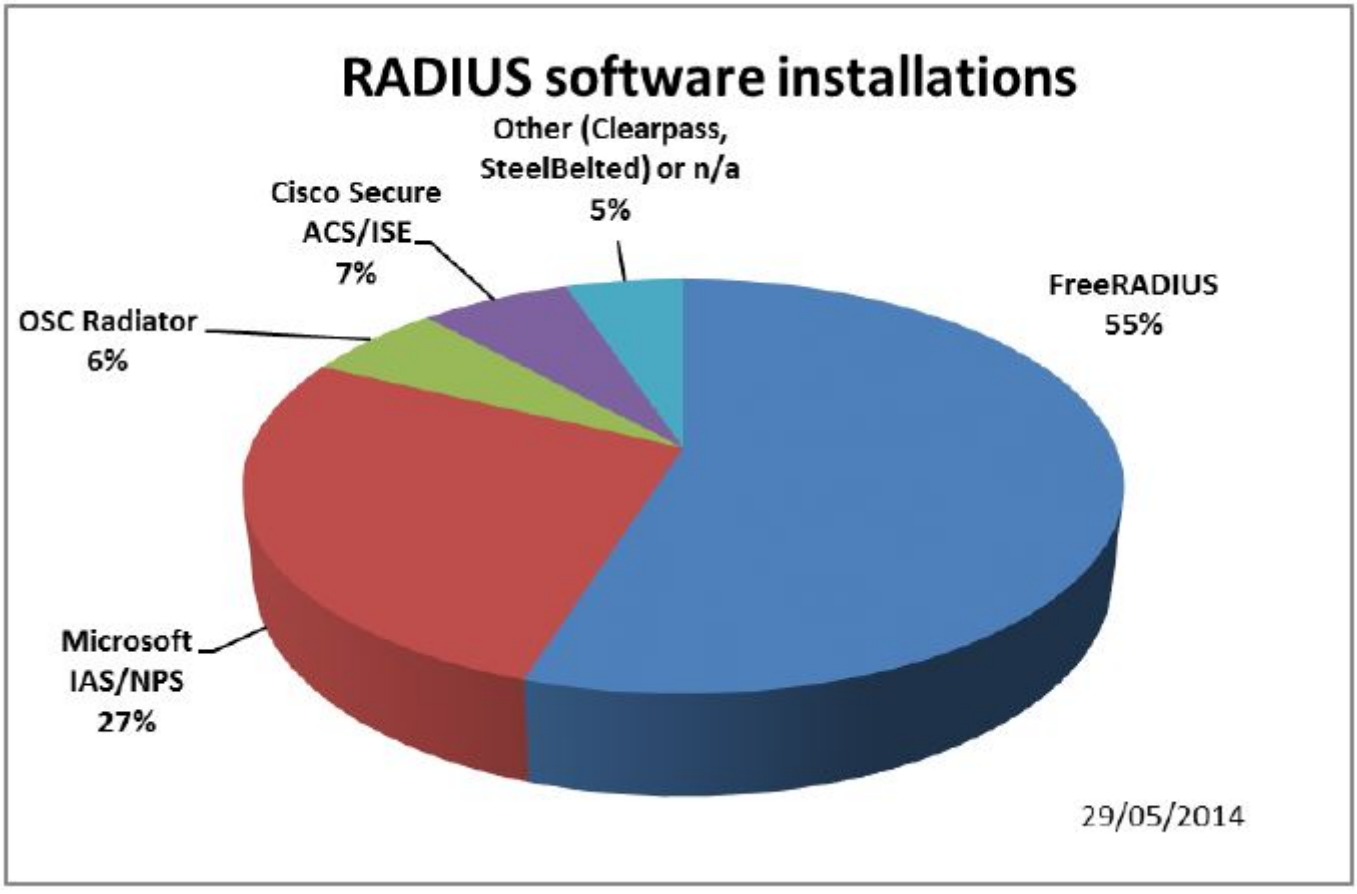
- Windows Server 2003, Standard Edition or Enterprise Edition (for IAS and Certification Authority (CA) installation). Standard edition supports maximum of 50 wireless APs (RADIUS clients) per server.
- FreeRADIUS - as many as your server can logically handle
- RADIATOR - as many as your server can logically handle
- CiscoACS - Number of Access Points. To determine the number of access points that a Cisco Secure ACS can manage, start with the assumption that each access point manages about ten WLAN users. Then divide the total number of users that can be supported by a Cisco Secure ACS - 21,000 by this number. With this formula we have 21,000 divided by 10 or 2,100 access points that can be supported by one Cisco Secure ACS. This is the minimum number of access points that can be supported because not all access points will be supporting the maximum number of users at any one time.
- Number of Network Access Servers - a Cisco Secure ACS can support up 5,000 discrete network access servers (NASs). This number can be increased by the use of the multi-NAS capability of an ACS. Multi-NAS is a concept that allows one or more addresses to be configured for a given NAS entry. Using multi-NAS, the Cisco Secure ACS can support a theoretical maximum of 255 multiplied by 5,000 discrete NAS equaling 1.275 million devices. However, a configuration of 1.275 million devices per Cisco Secure ACS is clearly not realistic.

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



[21]

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 software, including the following:

FreeRADIUS - version 3.0.22 is the current release at the time of writing https://freeradius.org/releases/ [22]

The 2.x.x release series is now End Of Life. Only security fixes will be applied to 2.x.x. Users of 2.x.x are encouraged to migrate to the latest 3.0.x series release. If you are using versions of FR before 2.2.10, upgrade to version 2.2.10 or 3.0.22. Release 2.2.10 was the final version of the 2.2.X product (which whilst end of life fixed many 1.1.x issues).

Archive note: Versions prior to 1.1.4 did not support 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.

Versions 1.1.3-1.1.7 were vulnerable to being crashed by an attacker sending a Tunnel-Password attribute in an Access-Request packet.

Use of the old 1.1.x code is deprecated, 1.1.8 was the final version of the 1.1.x product.

Further details regarding security vulnerabilities of FreeRADIUS versions can be found here: http://freeradius.org/security.html [23]

Radiator - in June 2007 the eduroam(UK) 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 4.4 is the latest version, last modified 11 March 2009).

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.

A full history of Radiator software revisions can be found here: Radiator Revision History [24]

Are there any example configurations for Radiator available?

We currently don't have any direct cut'n'paste for Radiator that is clearly available for any site due to the uniqueness of each site requirement (backend authentication and such).

However, OSC (the publisher of Radiator) has produced a number of example configuration file snippets and templates which can be found in the goodies directory on a Radiator server. Eg. ntlm_eap_multi.cfg is a simple config which handles Radius PAP, CHAP, MSCHAP and MSCHAPV2 and also handles the outer and inner requests for TTLS and PEAP. In this case, the <AuthBy NTLM> sub-handler is doing the work. (Of course this is only suitable for Active

Directory. If sites are using passwords or eDirectory etc then the requirements will be different).

Resources:

Also appendix A.2 of the Geant2 Roaming Infrastructure Service and Support Cookbook [25] provides useful information on configuring the ORPS server software.

Are there any example configurations for FreeRADIUS available?

We don't have any direct cut'n'paste configurations for FreeRADIUS that would be suitable for all sites due to the uniqueness of each site requirement (backend authentication etc).

However there are some hints and tips on the Support web site and there is some useful information in the following case study, which is a practical description of how University of Bristol implemented and complies with the Technical Specification using FreeRADIUS in an AD environment: A Case Study in Complying with the Technical Specification.

- Also appendix A.2 of the Geant2 Roaming Infrastructure Service and Support Cookbook [25] provides Roaming Technology - FAQsuseful information on configuring the ORPS server software.
- **FreeRadius website** **[15]**

What is unlang?

The unlang language available in FreeRADIUS takes flexibility in authorization to new heights. Unlang is not a full blown programming language, but rather a processing language. The purpose of unlang is to implement policies and not to replace complex scripts like those created with Perl or Python. Unlang sticks to a basic syntax that includes conditional statements and manipulation of variables. The unlang code does not get compiled but is interpreted by the FreeRADIUS server. The interpretation happens when the server reads the configuration files, which typically happens during start-up. The use of unlang is restricted to specified sections inside the configuration files and cannot be used inside the modules.

Source: https://www.safaribooksonline.com/library/view/freeradius-beginners-guid... [26]

Where can I get up to date binaries for FR2.2 for Centos (which ships with an old version)?

As of Jan 2015 CentOS 6.5 ships with 2.1.12, which is a somewhat deprecated version. I'm keen to get an up to date version. I'm loathe to compile from sources because we don't have the time to maintain manually compiled versions of things.

Try here:
http://software.opensuse.org/download.html?project=home%3Afreeradius%3A2.x.x%3Acentos&packag
[27]

What's the Difference between MS IAS and NPS?

Here's what msdn says - Internet Authentication Service vs Network Policy Server [28]. But we have also found difference in that IAS requires a workaround to be applied in order to avoid a problem related to Operator-Name

Microsoft IAS Deployment

- Basic IAS Installation and Configuration [29] (TechRepublic paper 2007)
- Microsoft IAS (Technet) [17]
- Deployment of 802.1X for Wired Networks Using Microsoft Windows [30]
- Deploying MS IAS with VLANs [31]
- MS IAS Operations Guide [32]

Microsoft NPS (Windows 2008/R2 and 2012/R2) Deployment

- 802.1X Authenticated Wireless Access (Technet) [33] - contains Design and Depolyment guide sub-sections
- Complete How to Configure Microsoft NPS (Technet) [34] - deployment as RADIUS authentication and RADIAS proxy server

Troubleshooting Microsoft IAS as a RADIUS server and as a RADIUS proxy

This link to the MS TechNet site should be useful:

- IAS Troubleshooting as a RADIUS server - Authentication Problems (Technet) [35]
- IAS Troubleshooting as a Proxy server - RADIUS Forwarding Problems (Technet) [36]

Our AD usernames don't match eduroam username format, how can I strip/modify realm for authentication?

Our usernames in AD just use the userID format not userID@realm [37] - how do I strip the realm prior to authenticaiton?

Our usernames in AD use a different realm (e.g. @ad.camford.ac.uk) - how do I modify the realm component?

The recommended solution is to add the required realm as a UPN in AD - this will allow NPS to authenticate the eduroam usernames against your AD.

See section 13 of https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-2 [38]

Cisco ACS Implementation

We have configured the relevant databases for our ACS servers and ports on the ASA firewalls, now we need some help in configuring ACS 4.0 for PEAP.

The following Cisco links give various bits of help regarding ACS and PEAP:

- PEAP under Unified Wireless Networks with ACS 4.0 and Windows 2003 [39]
- System Configuration: Authentication and Certificates [40]

When initially setting this up it is a good idea to maximise the logging as follows.

How to Set the Logging Level to Full in the ACS GUI:

You will need to set ACS to log all messages. To do this, follow the steps listed below:

1. From the ACS home page, go to Systems Configuration > Service Control.
2. Under the Service Log File Configuration heading, set the level of detail to Full.

You can also use the command line tools to further debug - there's a whole suite of them.

ACS Internal Architecture - CSTacacs and CSRadius [41]

CSRadius appears to be the most useful - for an example of it in action see:

Obtaining vs and AAA debug info for Cisco Secure ACS - RADIUS success authentication [42]

I've set up Attribute filtering - what Attributes should I NOT filter out?

The following is the minimum set of attributes required to support eduroam. These must not be filtered out:

RADIUS Access-Request or Access-Challenge message attributes:

1. User-Name
18. Reply-Message
24. State
25. Class
31. Calling-Station-ID
33. Proxy-State
79. EAP-Message
80. Message-Authenticator
    MS-MPPE-Send-Key
    MS-MPPE-Recv-Key
89. Chargeable-User-Identity
126. Operator-Name

RADIUS Accounting messages:

1. User-Name
25. Class
33. Proxy-State
40. Acct-Status-Type
44. Acct-Session-ID

This list has been determined following a small number of incidents involving Roaming users being unable to connect at certain institutions (both here in the UK and elsewhere) owing to over-restrictive attribute filtering. Please note that implementation of the list is likely to become a mandatory feature of eduroam.

If you are aware of any other attributes then please contact eduroam Support.

For more information on this topic see:

- List of RADIUS Attributes [43]
- RADIUS Attributes [44]
- Attribute Screening for Access Requests on Cisco Network Access Server [45]

What procedure do I need to follow for changing the IP address of our ORPS?

You need simply to use the https://support.eduroam.uk [46] support site. Go to your ORPS configuration page and select your ORPS, change the name of the RADIUS server and press [Update RPS]. Check that the passphrase does not change (it should not). The final step is to remove the old ORPS entry and add the new one. The passphrase will be different then. The changes are propagated to the NRPS on the hour.

How do I set the shared secret for ORPS in a fail-over cluster to be the same?

It is best practice to use one shared secret for each ORPS-internal RADIUS server pair. This is to limit the effect of one RADIUS server being compromised or having the credentials leaked giving further access to the rest of the RADIUS infrastructure. In some cases it is not feasible to have seperate shared secrets, for example in a system where the RADIUS servers have a shared/synchronised database.

In this case you can request eduroam(UK) Support to set the same set of shared secrets to be same for all you ORPSs.

IP Addresses/FQDNs/shared secrets for ORPS - replacing ORPS and moving to a new location

What is the recommendation regarding use of same or unique shared secrets for ORPS / internal RADIUS servers?

We have multiple internal RADIUS servers at departments and colleges, should be use separate shared secrets for each pairing or would a common one be acceptable?

It is best practice to use one shared secret for each ORPS-internal RADIUS server pair. This is to limit the effect of one RADIUS server being compromised or having the credentials leaked giving further access to the rest of the RADIUS infrastructure. In some cases it is not feasible to have seperate shared secrets, for example in a system where the RADIUS servers have a shared/synchronised database.

In this case you can request eduroam(UK) Support to set the same set of shared secrets to be same for all you ORPSs.

We don't think our ORPS are communicating with the NRPS properly although we've set the NRPS up as clients and configured forwarding. What's going wrong?

'Invalid message authenticator' type error entries may be seen in the NRPS Radius errors logs on your eduroam(UK) Support server Troubleshoot page or you may see similar error messages in your ORPS error logs (e.g. NPS event log)

***'Bad Authenticator' error entries are being seen in the NRPS error logs views on eduroam(UK) Support*:**

- Mon Oct xx xx:xx:xx 2014: WARNING: Bad EAP Message-Authenticator

- Mon Oct xx xx:xx:xx 2014: WARNING: Bad authenticator in request from xxx.yy.zzz.118 (xxx.yy.zzz.72))

'Message-Authenticator attribute that is not valid' error messages being seen in Microsoft NPS server error/event log:

- An Access-Request message was received from RADIUS client 194.83.56.233(*)
with a Message-Authenticator attribute that is not valid (*) any NRPS address

Bad authenticator in an Access-Request indicates that the shared secret is incorrect. So the log error entry indicates that an ORPS that has a incorrect shared secret configured for a NRPS. (Remember, each NRPS-ORPS pair has an individual shared secret).

If there is a further IP address in brackets in the error entry, this indicates that you might have an internal system with an incorrect shared secret with your ORPS. (Best practice is for each RADIUS pair on your internal network to have its own secrets). The NAS systems (APs, WLCs [switches if applicable], that talk to your ORPS internally need to have their own correct shared secrets. If your ORPS behaves badly and forwards RADIUS packets containing a bad EAP Message-Authenticator, the result will be that the NRPS detects the error, drops the packet and records the entry in the log - which is propagated to your view of the error log on eduroam(UK) Support.

Solution - correct your shared secrets on NASs and ORPS.

***'Unknown client' error entries are being seen in the NRPS error logs views on eduroam(UK) Support*:**

Unknown client means that the RADIUS client is unknown, the NRPS don't recognise the IP address of the RADIUS server that is sending authentication requests to them. This could be because you have not correctly added the ORPS details into the ORPS config screen on the Support server. Alternatively it could be that there is a DNS issue. You define your ORPS as a FQDN. If this is not correctly resolved or if your ORPS is using an address other than can be resolved, the NRPS will not reply and the unknown client error will be logged.

'Network Policy Server denied access to a user - reason code: 23 - An error occurred during the Network Policy Server use of the EAP protocol' error messages are being seen in the Microsoft NPS logs (a 6273 event is being logged)

This indicates a server certificate issue. The server must have a valid certificate and that certificate must be referenced in the connection request policy and the network policy that serve your clients (i.e. the local user connection policy and the user authentication policy).

The EAP log files on the server may reveal more detail.

Note that there are certain requirements pertaining to the server certificate - see https://wiki.geant.org/pages/viewpage.action?pageId=121346259#Howtodeplo... [47] (ADVANCED)-Consideration2:Recommendedcertificateproperties

In addition, the client device needs to trust the RADIUS server certificate and different client operating systems/Wi-Fi client software have differing requirements and configuration settings.

Does Microsoft NPS support RADIUS accounting and how to avoid forwarding accounting packets to NRPS?

Yes Microsoft NPS does indeed support RADIUS accounting. But by default NPS does not log any data - although you should be logging authentication events in order to comply with the eduroam(UK) Technical Specification. https://msdn.microsoft.com/en-us/library/cc725566%28v=ws.11%29.aspx [48] and https://technet.microsoft.com/en-us/library/dd197475%28v=ws.10%29.aspx [49]

By default NPS does NOT forward accounting packets, but it is possible to configure the server to do so!

Microsoft documentation states: ‘Connection request policy accounting settings function independently of the accounting configuration of the local NPS server. In other words, if you configure the local NPS server to log RADIUS accounting information to a local file or to a Microsoft® SQL Server™ database, it will do so regardless of whether you configure a connection request policy to forward accounting messages to a remote RADIUS server group.’

To comply with eduroam(UK) Tech Spec you need to ensure that you configure the local NPS server to log RADIUS accounting information to a local file or to a Microsoft® SQL Server™ database.

The May 2016 eduroam(UK) advisory notice requests that you ensure that you have NOT set a **connection request policy** to forward accounting messages to the NRPSs.

NB. A default connection request policy is created when you install NPS. This policy has the following configuration:

- **Authentication** is not configured.
- **Accounting** is not configured to forward accounting information to a remote RADIUS server group.
- **Attribute** is not configured with attribute manipulation rules that forward connection requests to remote RADIUS server groups.
- **Forwarding Request** is configured so that connection requests are authenticated and authorized on the local NPS server.
- **Advanced** attributes are not configured.

To learn about accounting and logging in NPS see:

https://msdn.microsoft.com/en-us/library/cc725566%28v=ws.11%29.aspx [48]

https://technet.microsoft.com/en-us/library/dd197475%28v=ws.10%29.aspx [49]

http://services.geant.net/cbp/Knowledge_Base/Wireless/Documents/CBP-13_Using-Windows-NPS-as-RADIUS-in-eduroam_final.pdf [50] (p.42 (section 6))

Further references:

https://msdn.microsoft.com/en-us/library/bb892012%28v=vs.85%29.aspx [51]

https://msdn.microsoft.com/en-us/library/cc753603.aspx [52]

https://technet.microsoft.com/en-us/library/dd197475%28v=ws.10%29.aspx [49]

6) Server Certificates for ORPS

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

Yes. The RADIUS server certificates required for most EAP methods used in eduroam may be self-signed / signed by private certificate authority (CA) or they can commercially provided and signed by a public CA such as Sectigo (which is the CA provider behind the Jisc Certificate Service).

EAP methods that use transport layer security (TLS), such as EAP-TLS, EAP-PEAP and EAP-TTLS, require the use of a server certificate to authenticate the RADIUS server to the supplicants. In addition EAP-TLS requires client certificates too in order for the clients to be validated by the RADIUS servers. These client certificates can be can also be self-signed, i.e. generated by your private CA software.

The advantages and drawbacks of both using private and public CAs are listed below.

Using a certificate from a self-signed private CA

Benefits:

- No need to purchase a certificate from a commercial vendor - saving cost.
- Eliminates the slight inherent security weakness implicit with commercially provided certificates when a client device is not configured to validate the certficate name (CN/SAN:DNS). A rogue RADIUS server used in a MITM attack, could present a valid cert from a commercial CA that would be trusted by the client device if i) the CA is the same as your actual RADIUS server and ii) the client device does not have certificate name validatation set. By you operating your own private CA, an attacker would find it hard to acquire a legitimate certficate. Note that CAT and geteduroam installers always configure proper cert validation c/w CN checking - which ensures security when a commercial CA is used.
- Long certificate expiry date can be applied.

Drawback:

- You will generally have to install or get the laptop user to install the ‘root certificate’ from your self-signed Certificate Authority on each client before it will recognise a private server certificate. This is not a difficult procedure with mobile device management

software for corporately managed devices, but may be more of challenge for users own devices. This is where the eduroam CAT system is invaluable.

Using a certificate from a commercial CA

Benefits:

- Avoids the complication of operating your own CA (which includes making CRL URL publicly accessible)
- No need to distribute the CA's root certificate to each client since public CA certificate will generally be recognised by any client, since such certs are distributed with operating systems.
- The correct extension attributes will be present (if requested or needed) - eliminating necessity of configuring openssl etc.

Drawback:

- Cost - you usually have to pay an annual fee for each certificate (although Jisc provided certs are very low cost)
- Slight vulnerability to illegal spoofing
- Requirement to renew the certificate annually

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:

- TechRepublic paper (2007) - Self-sign a RADIUS server for secure PEAP or EAP-TTLS authentication [53]
- Microsoft technical article - Certificate requirements when Using EAP-TLS or PEAP with EAP-TLS [54]
- Private certificate authority software

Can I use the Jisc Certificate Service to provide certificates for my RADIUS servers? / Do you have any technical documentation on using MS IAS and Jisc Cert Service?

Yes - the Jisc Certificate Service [55] works fine with the most popular RADIUS servers; FreeRADIUS, Radiator, Microsoft NPS, Aruba ClearPass and Cisco ACS and will provide you with server certificates at low cost - suitable for use with EAP-PEAP and EAP-TTLS methods.

[Historical note - the old Microsoft Internet Authentication Service (IAS) required careful configuration of the CSR to for use with JCS (Comodo) certificates - a tech guidance sheet was available].

Archive Note:

The difficulties with the old MS Internet Authentication Service stem from the fact that it does not send the full certificate chain during EAP-PEAP negotiation. Current NPS systems do send the full chain and there is not a problem. But in order to use the old IAS with Jisc SCS certificates (or any other certificate not issued directly from a certification authority (CA)

'known' by the supplicant), it was essential to:

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

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

This issue came to light through problems experienced in attempting to use certificates issued by the Jisc SCS with the Windows XP supplicant. All certificates issued by the Jisc SCS 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. Choose a vendor that will supply a certificate that will 'chain directly' to a root CA 'known' by your supplicants.

2. Be very careful and thorough in your configuration of IAS.

[Anyone considering use of Jisc SCS certificates should read the Janet guide - Using Certificates Issued by the Jisc SCS with MS IAS.]

3. Manage your own private CA.

What do we need to configure on client workstations in order to use the TERENA certificates supplied through the Janet/Jisc Certificate Service?

DRAFT ANSWER!

Windows (and other OSs) only natively trust certain certificate CAs for 802.1X. The certificates provided by Jisc used to be supplied by Comodo (UTNAddTrustServer_CA, TERENASSLCA and AddTrustExternalCARoot) but are now supplied by QuoVadis.

Is there a way around this without the end user having to configure their advanced wireless settings?

Old Comodo certificates supplied through TERENA under the Jane/Jisc Certificate Service:

USER Trust - UTN-USERFirst-Hardware-TERENA SSL CA

AddTrust External CA Root is in the Windows default list. Have you ticked this CA in the list of Trusted Root Certification Authorities in the PEAP properties.

The Jisc Certificate Service now (April 2015) of course provides QuoVadis certificates and you need to use the appropriate CA as the Trusted Root Certificataion Authority

Can I use the same certificate for more than one ORPS?

Yes you can indeed use the the same certificate for more than one ORPS. In fact it's better to do this because then there will be only one CN /SubjectAlternativeName:DNS for the client devices to be configured with. You can also save the cost of additional certificates. When

creating your CSR be sure to make the private key it exportable. The signed server certificate received from your chosen CA can then be exported and copied and imported into subsequent RADIUS server c/w the key.

Archive item - 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) [56]

Are there any likely issues for users when we replace our JCS-supplied ORPS server certificate?

This section is due for an update.

Our ORPS server certificate is due to expire shortly and we have a replacement JCS certificate which uses the identical three intermediate certificates in our old certificate (Addtrust, UTN and Terena CA). Users have been using eduroam profiles created using the cat.eduroam.org installer. The question is: Will there be any impact on users if the latest radius certificate is applied on our end (authentication) servers?

There shouldn't be any issues if users have configured their device correctly to trust the CA and only the CN of the ORPS server. By contrast, clients in which the set up process has been shortcut by just entering username and password after clicking on 'connect to eduroam' will have problems. This is because devices often install the RADIUS server cert and trust only that certificate when the user just clicks on the SSID and enters their username and password.

Our ORPS server certificate is about to expire, what do we do?

If the new certificate is just a renewed version of the old one, signed by the same root CA then the trust installed on end user devices will still work and all you need to do is replace the old certificate file with the new one. See http://docplayer.net/13268335-Server-certificate-practices-in-eduroam.html [57]

If you are using a new CA, or the CA has changed its root certificate in the mean time, you will need to update the root CA installed with the eduroam profile in end user devices. For most devices you can install a second root CA in the profile in advance so it doesn't need to happen on switch date all at once. Some android devices don't have support for multiple roots in a profile so these will need to be updated after the switch. See the 'CA rollover support' section in https://wiki.geant.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+institution+administrators [58]and https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations [59]

7) Integration of RADIUS Server with Back-end User Database

Is it possible to authenticate EAP-PEAP against Novell Directory Services?

While it is not possible to authenticate EAP-PEAP against the default non-reversible hash used in NDS, it is now possible to configure a "Universal Password" in NDS which stores users' passwords in a reversibly encrypted format. This will permit the authentication of EAP-

PEAP against NDS through RADIUS servers such as FreeRADIUS and Radiator.

How do you configure FreeRADIUS against Novell eDirectory?

Novell has produced documentation on configuring FreeRADIUS against eDirectory:

http://www.novell.com/documentation/edir_radius/index.html [60]

FreeRADIUS integration with Active Directory

The received way of setting up FreeRADIUS to authenticate users against Active Directory is to use Samba/winbind/ntlm_auth:

FreeRADIUS Active Directory Integration Howto - from FreeRADIUS Wiki [61] (Login required)

University of Bristol implemented FreeRADIUS in an AD environment. The following case study contains useful information: A Case Study in Complying with the Technical Specification.

Radiator integration with Active Directory

The first thing to note is that different handlers in the radius.cfg should be used dependent on the OS platform of your Radiator server. AD is also problematic as it will not permit access to plaintext password by the RADIUS server.

There are a large number of sample configuration files and templates in the 'goodies' directory on Radiator servers which should prove helpful. These can be modified to suit your environment with options configured such as domain name, IP addess, password etc.

Realm name not in AD - can we get NPS to translate realm?

You cannot manipulate the realm with NPS - this is something that you used to be able to do in the IAS days, but on all modern clients it will cause EAP to fail because the MPPE key derivation is from the original client-provided username, not from what a RADIUS server might turn it into. You shouldn't be attempting to manipulate the realm though - if AD is your backend then you actually just need to add the realm in question to the AD as another global UPN - NPS in AD will then just handle it.

You can read more here: https://social.technet.microsoft.com/Forums/windowsserver/en-US/e73183d4-7b2f-48a7-9246-97ed711e8e8d/eappeapmschapv2-realm-stripping?forum=winserverNAP [62]

Links
[1] http://community.jisc.ac.uk/library/advisory-services/ieee-8021x
[2] http://community.jisc.ac.uk/library/advisory-services/extensible-authentication-protocol
[3] http://technet.microsoft.com/en-us/library/jj125379.aspx
[4] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap
[5] https://community.jisc.ac.uk/library/janet-services-documentation/eduroamuk-technical-specification
[6] https://jisc365.sharepoint.com/:b:/s/PublicDocumentLinks/EYNd3t02k8hGhsEC8K2f338BnKEO5Nrm5b-0aJmdbWgwrw?e=tbytM4

[7] https://www.howtogeek.com/179089/lock-down-your-wi-fi-network-with-your-routers-wireless-isolation-option/
[8] https://community.jisc.ac.uk/library/janet-services-documentation/faqs-eduroam-system-administrators-and-implementation-techs-0
[9] https://www.helpnetsecurity.com/2017/03/08/https-interception-dilemma/
[10] https://community.jisc.ac.uk/blogs/regulatory-developments/article/gdpr-whats-your-justification
[11] http://www.firewall.cx/networking-topics/network-address-translation-nat/233-nat-overload-part-1.html
[12] https://community.jisc.ac.uk/library/janet-policies/eligibility-policy-guidance
[13] https://community.jisc.ac.uk/library/janet-policies/guest-and-public-network-access
[14] https://community.jisc.ac.uk/library/janet-services-documentation/clarification-eduroamuk-policy-and-tech-spec-wording-visitor
[15] http://www.freeradius.org/
[16] http://www.open.com.au/radiator/index.html
[17] http://technet.microsoft.com/en-us/network/bb643123.aspx
[18] http://technet.microsoft.com/en-us/windowsserver/dd448603
[19] http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html
[20] http://www.juniper.net/products_and_services/aaa_and_802_1x/steel_belted_radius/
[21] https://community.jisc.ac.uk/system/files/public_images/RADIUS software installations chart 14_05_29.JPG
[22] https://freeradius.org/releases/
[23] http://freeradius.org/security.html
[24] http://www.open.com.au/radiator/history.html
[25] http://www.eduroam.org/downloads/docs/GN2-08-230-DJ5.1.5.3-eduroamCookbook.pdf
[26] https://www.safaribooksonline.com/library/view/freeradius-beginners-guide/9781849514088/ch07s03.html
[27] http://software.opensuse.org/download.html?project=home%3Afreeradius%3A2.x.x%3Acentos&package=freera
[28] http://msdn2.microsoft.com/en-us/library/bb892033%28VS.85%29.aspx
[29] http://www.techrepublic.com./article/ultimate-wireless-security-guide-microsoft-ias-radius-for-wireless-authentication/
[30] http://www.microsoft.com/downloads/details.aspx?familyid=05951071-6b20-4cef-9939-47c397ffd3dd&displaylang=en
[31] http://www.microsoft.com/en-us/download/details.aspx?id=11201
[32] http://www.microsoft.com/downloads/info.aspx?na=47&p=4&SrcDisplayLang=en&SrcCategoryId=&6b20-4cef-9939-47c397ffd3dd&u=details.aspx%3Ffamilyid=27C432BF-5ED0-4763-8909-36E7C310AE3C&displaylang=en
[33] http://technet.microsoft.com/en-us/library/cc771455(v=ws.10).aspx
[34] http://technet.microsoft.com/en-us/library/d80d8fd1-388f-49e1-8b32-855cf8fda137
[35] http://technet.microsoft.com/en-us/library/cc786978(v=ws.10).aspx
[36] http://technet.microsoft.com/en-us/library/cc780788(v=ws.10).aspx
[37] mailto:userID@realm
[38] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-2
[39] http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a00807917aa.shtml
[40] http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/sau.h
[41] http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.0/user/guid
[42] http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_tech_note09186a00800afec1.shtml#rad_good_a
[43] http://www.freeradius.org/rfc/attributes.html
[44] http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/A_RADAtr.
[45]

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_att_scrn_accreq_external_docbase_0900e4b
[46] https://support.eduroam.uk
[47]
https://wiki.geant.org/pages/viewpage.action?pageId=121346259#Howtodeployeduroamonsiteoroncampus
[48] https://msdn.microsoft.com/en-us/library/cc725566%28v=ws.11%29.aspx
[49] https://technet.microsoft.com/en-us/library/dd197475%28v=ws.10%29.aspx
[50] http://services.geant.net/cbp/Knowledge_Base/Wireless/Documents/CBP-13_Using-Windows-NPS-as-RADIUS-in-eduroam_final.pdf
[51] https://msdn.microsoft.com/en-us/library/bb892012%28v=vs.85%29.aspx
[52] https://msdn.microsoft.com/en-us/library/cc753603.aspx
[53] http://www.techrepublic.com./article/ultimate-wireless-security-guide-self-signed-certificates-for-your-radius-server/
[54] http://support.microsoft.com/kb/814394
[55] http://www.ja.net/jcs
[56] http://www.microsoft.com/downloads/details.aspx?familyid=1971D43C-D2D9-408D-BD97-139AFC60996B&displaylang=en
[57] http://docplayer.net/13268335-Server-certificate-practices-in-eduroam.html
[58] https://wiki.geant.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+institution+administrators
[59] https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations
[60] http://www.novell.com/documentation/edir_radius/index.html
[61] http://wiki.freeradius.org/FreeRADIUS_Active_Directory_Integration_HOWTO
[62] https://social.technet.microsoft.com/Forums/windowsserver/en-US/e73183d4-7b2f-48a7-9246-97ed711e8e8d/eappeapmschapv2-realm-stripping?forum=winserverNAP