FAQs for eduroam System Administrators and Implementation Techs - Part 2

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 1 is your question is not addressed here.

Last Updated 03/02/2025

Contents

- Notification of Home organisations in case of visitor abuse of Policy
- Dealing with a virus incident involving an eduroam visitor

5) RADIUS Server log Keeping, Interpreting Errors in the ORPS logs and Performance Difficulties

- Generation of Monthly Stats on eduroam usage for Microsoft IAS/NPS
- Microsoft NPS Error 'RADIUS Client Authentication Attribute not Valid' (ID 18)
- Microsoft NPS Error 'Wrong Domain' (ID 4402)
- Aruba Clearpass authentication rejection Error code 204 'Failed to classify request to service'/'Service Categorization Failed'
- Peaks of re-authentications at certain times of the day/heavy auth load leading to failures and poor performance
- Where to find FreeRADIUS authentication logs

6) eduroam(UK) Support Server / ORPS-related Questions

- Do we need to give our ORPS a FQDN; can't we register the ORPS simply by its public IP address?
- Making a change to the IP address of an ORPS
- IP address of ORPS displayed on Configuration page of eduroam(UK) Support server still shows old address some time after making the change in DNS
- What category of RADIUS client to use for a server acting as proxy to the NRPS but not from the NRPS (to act as gateway to a 3rd party associate organisation)?
- How often is the sites information entered in the Support server uploaded to the eduroam locations map http://monitor.eduroam.org/gmap/country.php?country=uk [1]?

7) eduroam(UK) Support Server Tests and Testing

- Facility for stopping production traffic going to an ORPS during testing and routing only test traffic to ORPS under test
- Support server EAP-TTLS(PAP) test use of null outer id causing errors to be logged
- 'PEAP-MSCHAPv2 authentication failed: IPv4, RFC realm name' Detected Issue error message on Status Summary and ORPS config pages on Support server
- Simulated visitor test fails but remote authentication test works/authentication for visitors fails but our users can roam ok
- How can we test our implementation of CUI; does the simulated visitor test enable CUI to be tested?
- Remote authentication test fails but simulated visitor test works
- Why is the Support Server test system only testing access to one of our multiple ORPS?
- Why are we getting errors logged every 5 minutes after having changed our eduroam(UK) configuration on the Support server
- What does the error condition 'HTTP CRITICAL - pattern not found' mean in the Nagios LG monitor for our site?
- Why do I get only "Re-sending Access-Request" when testing authentication via the support server?
-

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

8) Upgrading FreeRADIUS from v 1.1.x to v2.0.x

- Guidance on upgrading to FreeRADIUS 2.0.x

9) Visiting User Authentication Problems / Firewall configuration

- Why do I get "re-sending Access-Request" when testing remote authentication?
- Why do we appear to not be getting any response from the eduroam NRPSs when visitors try to authenticate?

10) Wired Networks

- How do you configure a Cisco Catalyst switch to operate with 802.1X?

1) 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 was the CA provider behind the Jisc Certificate Service).

With EAP methods that use transport layer security (TLS), such as EAP-TLS, EAP-PEAP and EAP-TTLS, the server certificate is used 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 your own 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:

- Since the self-signed ‘root certificate’ of your Certification Authority won't have been installed into user devices at the time of manufacture along with the device operating system, your CA root certificate will generally have to be installed into client devices' trust stores using desktop management systems (e.g. Intune) or by manual installation by the user or by using a device setup provisioning system. This will be essential to enable the client device to trust a server certificate issued by a private CA. 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

Which solution to choose depends on individual organisation circumstances - either option is valid, although if maximum certificate validity periods for commercial CA certs is reduced from the current 12 months, the incentive to pite the bullet and operate your own CA will increase!

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 [2]
- Microsoft technical article - Certificate requirements when Using EAP-TLS or PEAP with EAP-TLS [3]
- Private certificate authority software

Can I use the Jisc Certificate Service, which now supplies Sectigo certs in place of QuoVadis ones, to provide certificates for my RADIUS servers?

Yes - the Jisc Certificate Service [4] 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.

The certificates supplied through the Jisc Certificate service are from Sectigo. i.e. the Geant/Comodo Certification Authority (CA). The certificates delivered through the Sectigo cert-manager portal have a relatively long chain of intermediate CAs before the top level root certificate authority is reached: server cert (e.g. camford.ac.uk) – GEANT OV RSA CA 4 - UserTrust RSA Certification Authority – Sectigo (Comodo AAA). So there is scope for errors to be made and for sub-optimal deployment. You will need to give some thought as to which certificates to install in your RADIUS server and to upload to the complementary CAT system, which generates EAP profiles for your users devices to facilitate setup and is strongly recommended for user device setup provisioning.

To download your server certificate and the various certification authority intermediate CA and root CA certificates you can use the Sectigo portal or the links in the e-mail from Certificate Services Manager sent when you enrolled your certificate. Options include downloading your certificate on its own, with the issuer chain and the issuer CA certificates themselves.

Before creating the CSR on your RADIUS server, the certificate consideration table on https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations [5] should be read for guidance. If using the Jisc Certificate Service, you'll be able to upload your CSR and download the server certificate and the Geant OV RSA CA 4 intermediate via the Sectigo portal. (OV certificates are recommended but EV certificates may be used, but add no benefit, take longer to deliver and can cause problems on some devices).

The Geant OV RSA CA 4 intermediate is issued by UserTrust RSA Certification Authority. There are both root and intermediate CA versions of this UserTrust certificate. And both validate the server certificates supplied from Sectigo, but to reduce complexity and eliminate potential issues on certain user devices we recommend that you use the root CA version of UserTrust. You'll need to download the root CA version via https://crt.sh/?id=1199354 [6]

What certificates to upload into the CAT system?

Ref: https://community.jisc.ac.uk/library/network-and-technology-service-docs... [7]

We recommend that the user device contains the following - hence you should upload the following into your EAP profile on CAT:

- the certificate of the intermediate CA that issued the server certificate
- the root CA certificate of the issuer of the intermediate certificate

i.e. If using the Jisc Certificate Service, the Geant OV RSA CA 4 intermediate and the *root* version of the UserTrust RSA Certification Authority

Nb. Whilst it may technically sufficient for the server to present only the server certificate if the user devices have both the root and intermediate(s) or for the device to only have the root CA certificate if the intermediate CA certificate is presented by the RADIUS server, the 'belt and braces' approach above is recommended.

Nbb. that the Secitgo portal delivers the *intermediate* version of the USERTrust RSA Certification Authority CA certificate. You should use the root version of this certificate in uploads into the CAT system. The root version is available at https://crt.sh/?id=1199354 [6]

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

DRAFT ANSWER!

The certificates provider for the Jisc Certificate Service has changed over time. Originally Jisc (Ukerna as it was then) supplied cetificates from Comodo (UTNAddTrustServer_CA, TERENASSLCA and AddTrustExternalCARoot). This provider was superseded by QuoVadis (in the days of Janet). And now Jisc has joined the pan-Europe Geant procurement scheme and provides Sectigo certificates.

Windows (and other OSs) only natively trust certain certificate CAs for use with 802.1X authentication.

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.

You will need to use the appropriate Sectigo 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 there will be only one CN /SubjectAlternativeName:DNS needed in the configuration of client devices. If using the CAT system, your EAP profile can be kept simple with just the one entry for CN name. You can also save the cost of additional certificates. When creating your CSR be sure to make the private key 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 - Do you have any technical documentation on using MS IAS and Jisc Cert Service?

Archive Note:

[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].

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.

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) [8]

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.

2) 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 [9]

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 [10] (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 [11]

3) Authentication Issues

Why should a Home organisation permit anonymous outer identities to be used?

The most often depolyed EAP methods are based on username and password. The majority of these (i.e. PEAP/MSCHAPv2, EAP-TTLS/*, EAP-FAST) use a two-stage authentication process and in each stage the user identity has a vital role. (EAP-TLS is certificate based and is not a two-stage process). The identity in stage one (e.g. the PEAP stage) is referred to as

the 'outer identity' and the identity in the second stage is referred to as the 'inner identity'.

In eduroam, usernames are required to be of the form 'userID@realm [12]'. In the first stage of authentication, it is only the realm component of the 'outer identity' username that is used by RADIUS proxy servers. The realm is used to establish the link between the client device and the user's home RADIUS server and enables visited site and national RADIUS proxy servers to forward the authentication request to the RADIUS authentication server for the user's Home organisation. In the user's home RADIUS server the outer identity realm may be used to determine how an access-request is handled (forwarded to another RADIUS server or passed to an authorisation process/policy). In the phase 1 stage, the userID in the outer identity plays no part. At the transition to phase 2 an encrypted tunnel is set up through which cryptographically protected 'inner identity' username and password are passed for the actual authentication of the user - and it is here that the userID is important.

In phase 2 it is generally **only** the userID component of the 'inner identity' username that is used for the actual authenticatication of the user against the user directory (AD/LDAP). In this user authentication phase, the authentication server is not normally concerned with the realm component of the username and it discards the realm component prior to the lookup against the user directory (AD/LDAP).

The above results in the possibility for the userID during the phase 1 stage of authentication to be obscured or witheld, for example the userID could be 'anonymous', 'fred.smith' or null. However this depends entirely on the Home RADIUS server being configured to allow the phase 1 identity to have a username with an anonymous userID. Whether or not you implement this for authentication of your own users on your RADIUS server is a matter for you to decide.

Note - RFC 4282 permits the use of anonymous outer identities the aim of which is the better preservation of privacy for your users. Since visitors to an organisation providing an eduroam Visited service may or may not have adopted an anonymous outer identity, the RADIUS server configuration for a Visited service MUST permit the use of anonymous/blank userID.

In relation to Home services, we recommend that your RADIUS server configuration SHOULD permit the use of anonymous/blank userID in the outer identity, i.e. the value the user inputs when enabling 'Enable Identity Privacy'/ 'Anonymous identity'. However this is a matter for the organisation to decide - it is not mandatory for you to allow use of anonymous/blank outer identity. Equally, eduroam(UK) does not mandate that anonymous/blank be applied in the outer identity. In fact for troubleshooting work, e.g. in the analysis of logs, it helps if outer identities are NOT anonymous.

In summary:

Visited services - MUST permit authentication requests that have an anonymous/blank userID in the outer identity to be forwarded to the NRPS.

Home services - SHOULD permit the use of anonymous/blank userID in the outer identity but are not required to.

Home services - are advised against enforcing or encouraging the use of anonymous outer identities.

Is 'machine authentication' permitted a) for roaming users b) for devices that will only connect on campus/at corporate office?

a) No, machine-based authentication (using usernames in the form 'domain\hostdevice') for machines roaming away from your own campus via eduroam is not permitted. eduroam policy states that the username needs to be in NAI format - ie userID@realm [12]. 'Machine authentication' is usually based on the utilisation of non-RADIUS-routable usernames in the form 'domain\hostdevice' so use of this format of credential is not possible technically in any case. eduroam policy requires that roaming authentications are based on the authentication of an individual identifiable and traceable user. If credentials such as deviceID@realm [13] (e.g. with a cached password) were to be used, whilst RADIUS-routing is possible, the user of the device could not be verified (note that secondary authentication is not permitted nor supported in eduroam) and it would not be possible to track down any individuals using the machine should there be a breach of Janet security policy. Hence machine-based authentication using credentials such as deviceID@realm [13] is not permitted when roaming.

b) However for devices that will only connect on campus/at corporate office, yes you may do machine auth on your own campus - with the proviso that you have the means to track down any individuals using the machine should there be a breach of Janet security policy. In practice this means that a device you want to machine-authenticate should be assigned to a responsible user. For on-campus-only use in cases where username/password credentials are utilised, such machines will not normally have RADIUS-routable usernames (for instance the username would be in the form 'device@camford.local [14]'), although where certificate based authetication is utilised devices would normally be identified with more usual username ' device@realm [15]'.

Can we utilise generic eduroam accounts for corporate devices we issue to registered staff/post-grads/students where we record which device is issued to which user?

Logging of user connection/activity would still be identifiable because the MAC address of the device issued to each individual would be recorded in our library management system.

eduroam(UK) policy requires that the spirit of the Janet Security and AUP are complied and moreover use of the Janet network and connection to it require adherence to those policies. eduroam logging policy requires that the individual is traceable if necessary, so the use of uniquely assigned credentials and logging of connection event time, IP addess, MAC address and user credentials are in general the logging requirements. If generic credentials are used, the individual can still be identified through the MAC address-user record (although MAC addresses can be spoofed). It is therefore acceptable for generic credentails to be used in the above scenario.

How can I differentiate between Institution-owned/managed devices and user-owned devices, (I want to manage the network environment they connect to after user authentication)?

One method to identify which auth requests come from institution-owned devices is to use the wireless MAC address of the device, which is included in the Calling-Station-Identity attribute in the Access-Request. Then to manage the network environment the authenticated user's device is connected to, do dynamic VLAN assignment.

Devices with MAC addresses known to belong to institution-owned/managed devices could be connected to your corporate network and unknown ones could be connected to your BYOD (insecure network for home-organisation users). Authenticated visitors should of course by placed onto your proper eduroam VLAN network. All of the above can be achieved through a single 'eduroam' SSID.

MAC addresses of course can be spoofed, so this is not method cannot be guaranteed to be 100% secure.

Another method would be use a certificate-based authentication mechanism, ie EAP-TLS. By setting certain parameters in the client certificates issued to institution-owned devices, your ORPS can be made aware of the category of device and return the relevant attribute to result in the device being connected to the required VLAN on your network.

When network passwords are changed the cached credentials on user devices have to be manually updated which sometimes creates issues for users

If using a password-based mechanism this is typically the case. Clients are dumb and some won't understand why an authentication request has failed after a central password change. However, there are ways of sending a request from the RADIUS server if the password is incorrect to make the client re-prompt the user for a password - that's IF the client supports such a prompt and the RADIUS server supports the mechanism.

Can't get Visited service to work - NRPS do not appear to be responding at all/ignoring all our ORPS/blocking auth requests

NRPS may appear to not be responding to authentication requests for a number of reasons:

- there could be a peering issue between the NRPS-ORPS
- a network or firewall issue may be preventing the auth requests from your ORPS reaching the NRPS
- your ORPS may not actually be sending auth requests to the NRPS
- if only some auth requests appear to be ignored the problem will be due to an issue at the visiting user's home site

RADIUS peering issues preventing the NRPS from responding to requests that it receives:

1) the server contacting them is not registered

2) the ORPS is registered but the shared secret is incorrect

Incorrect shared secrets are always logged as errors on Support Server and you will see these in the RADIUS errors log on the Troubleshoot page. With unregistered hosts it can be difficult to know which organisation they belong to so if your RADIUS server is not registered in Support you will only see them in your logs on the Support Server IF we can pick up enough info from the rDNS and WHOIS records.

Note that firewall issues may also result in the symptom that the 'NRPS are not responding'

If only some auth requests are ignored, this indicates either that the visitor's home ORPS is not responding or the authentication request contains an invalid realm name.

Your ORPS may not actually be sending auth requests to the NRPS or it may be only sending some

The NRPS may in fact be forwarding auth requests to visiting users home ORPSs but no response is returned. This could be due to the remote ORPS not returning an access-reject in cases where the realm is not being handled properly bu the remote ORPS or there is a user account issue or there could be a network problem.

CAT/geteduroam doesn't work for iOS but does for Android, why? (I've used separate certs on my ORPSs/a wildcard CN)

Q: Trying to use geteduroam, (having created a profile on CAT), App installs just fine and correct credentials are entered but:

- *With IOS devices, authentication fails*
- *With Android devices, authentication succeeds*

We are using separate certificates on our ORPS, each has a different CN name and matching subjectAltName: DNS (smith.camford.ac.uk and jones.camford.ac.uk) - so we've just put our domain name (camford.ac.uk) into the CAT profile since that is common between the ORPS certificates. This evidently allows Android to validate our server certs, but iOS just fails.

A: There is no common agreed method between operating system vendors (Apple, Android publishers, MS Windows, Linux, macOS) on how to validate server certificates. Android effectively uses the value provided as a wildcard (so a CAT profile with cert CN of *.camford.ac.uk would also work) whereas Apple does not allow this; with Apple, explicit names need to be provided.

To avoid this type of error we always recommend copying your server certificate and installing copies onto all of your ORPSs - this allows you to keep your CAT config simple.

4) <u>eduroam Policy Related Issues and Dealing with Virus/Copyright Breach Incidents</u>

Can you clarify Jisc's eduroam(UK) Policy/Tech Spec on vistor logging?

Clarification of eduroam Policy and Tech Spec Wording - Visitor Activity Logging.

In cases of major abuse by visiting guest eduroam users, who should we contact?

(By major abuse we mean those about which we receive a complaint from an outside organisation).

Fortunately such cases are few and far between, however if you receive a complaint from an outside organisation about a guest user on your network (eg. illegal copyright download notice), the user's Home organisation should be contacted immediately.

In the first instance you should try to contact the eduroam technical administrator at the Home site AND also please copy in Jisc Service Desk [16] quoting 'eduroam' in the subject line. Contacts are listed on the eduroam Support Server General Information [17] page. If you have difficulties in tracking down the administrator at the Home site (eg. in cases of visitors from outside the UK where searching on the eduroam.org site has been unfruitful), please contact Jisc Service Desk [16] and we will pursue the matter with eduroam.

Say we receive notification from Jisc CSIRT about suspected virus activity giving an IP address which turns out to be used by an eduroam visitor at our site, what do we do about it?

So CSIRT detects virus-related activity coming from your visited site and notifies you giving the IP address of the offender (who may be an eduroam user) and the date/time of the incident. You need to determine the MAC addess and probable home organisation of the offender using your detailed DHCP and RADIUS logs and you should then contact the home organisation to report the incident.

Obtaining MAC address and probable home organisation details:

Given the IP address CSIRT provides, your DHCP log should reveal the MAC address of the offender. The RADIUS log includes user-name, acct-session-id and calling-station-id attributes. Again, by using the IP address, the MAC address should be evident from the calling-station-id attribute and this should match the address revealed from the DHCP log.

You will be able to provide the probable realm name of the offender (from the user-name record, which can only be used to determine realm since the visited site RADIUS log only shows details of the outer ID/stage 1 authentication of an EAP authentication - which will be null@usersiterealmname.ac.uk [18] or anonymous@usersiterealmname.ac.uk [19] or realfred@usersiterealmname.ac.uk [20] in case of WindowsXP and Vista supplicants. Only the inner ID/stage 2 authentication utilises the real user ID). Nb. we cannot be certain that the indicated realm name is a definitive pointer to the realm of the real user ID since due to erroneous set up of proxying by some sites, the inner ID may be proxied off to another organisation for final authentication (we run a scan once a month to expose such errors).

Action:

The probable home site should now be contacted for details about who that user was (using date and time stamp details from the visited site logs, the home site should be able to track down the user and deal with the incident). The eduroam technical contacts/site eduroam administrators are listed here: https://support.roaming.ja.net/?q=general [17]

What should we do if we identify a virus infection on a visiting user's laptop if they are still on our eduroam guest network - do we have the right to block their access (based for example on MAC address of the Calling-Station-ID) or do we report this to eduroam Support (which will then escalate to the Home institution to deny authentication)?

If a visitor has a device with a proven virus infection or they breach yours or the Janet AUP then you should indeed block their access to your guest network. As service provider, you are certainly have the right to block access. You should however have a mechanism by which they know that they have been blocked for that reason - eg some captive page or network walled garden that gives them that information.

The case must also be escalated to the Home institution AND eduroam Support. Note that the visitor could be from a non-UK organisation so by notifying eduroam Support the issue will be pursued with eduroam.

Also note that whilst blocking MAC address is a simple method of denying access it could be circumvented if the visiting host is intent on more malicious activity (likewise, blocking on outerid won't be effective either).

5) RADIUS Server log Keeping and interpreting Errors in the ORPS logs

Keeping RADIUS logs is a requirement of the Technical Specification and we strongly recommend routine inspection of the RADIUS logs in order to reveal any underlying issues that may not be causing an obvious degradation of the service, but which will nevertheless be having an adverse effect on performance.

Generation of Monthly Stats on eduroam usage for Microsoft IAS/NPS

We've been asked to provide monthly stats on the number of internal and external users of our eduroam service, which is built on MS NPS. Is there an easy means of doing this?

Analysing/filtering the log files on the NPS servers is proving difficult since these are used for authentication by multiple SSIDs).

You will need to either parse logs or configure your ORPS/RADIUS server to log to a dB or file. If your system cannot log auth accept/fails to a separate simple log or an external dB then parsing of its internal/local log will be your only option. There is a Microsoft TechNet article which addresses this: http://technet.microsoft.com/en-us/library/dd197475(WS.10).aspx [21]

Errors in ORPS logs

Microsoft NPS Error 'RADIUS Client Authentication Attribute not Valid' (ID 18) appearing in our logs. What is causing this?

This error message indicates an incorrect shared secret. To fix this look at which RADIUS client (AP / Controller / RADIUS Proxy etc) is causing the error and check the match of the shared secret. Remember that if you have multiple ORPSs, and did not set the option to copy shared secrets when you registered each additional server, each ORPS-NRPS combination will have a different shared secret (this is the default options). Also, the RADIUS client causing the issue may be one of your own RADIUS clients on your network - if you only have

one ORPS and there are no issues detected and flagged up on the Status page on Support server or you can perform successful test user auth tests from the Troubleshoot page via all three NRPSs, this indicates the shared secrets with the NRPS are fine. Microsoft TechNet article on this: Access-request message received with authenticator attribute not valid. [22]

Microsoft NPS Error 'Wrong Domain' (ID 4402) appearing in our logs. What is causing this?

This error indicates that a domain controller can't be found for an authentication request from one of your RADIUS clients. You are receiving a request, which you aren't forwarding to the NRPS, but there's no domain controller available to handle the request. To investigate further you need more details about the error instances, i.e. for which domain a controller cannot be found. Microsoft TechNet article on this: There is no domain controller available for domain. [23]

Aruba Clearpass authentication rejection Error code 204 'Failed to classify request to service'/'Service Categorization Failed'

Aruba Clearpass authentication rejection error code 204 Authentication failure, Failed to classify request to service, Alert: RADIUS – Service Categorization failed.

Our Clearpass system is rejecting authentication attempts by roaming users whose accounts are definitely valid and whose credentials are definitely correct. The Request Details in the log states: Service Categorization failed. The user is authenticated okay on campus.

Check the conditions you have set in the Service Rule.

It would be normal to have a condition such as:

Type = Connection, Name = Src-IP-Address, Operator = BELONGS_TO_GROUP, Value = eduroam proxies

It would be wrong to filter on non-mandatory attributes that may not included by a Visited sites, such as:

Type = Radius:IETF, Name = NAS-Port-Type, Operator = EQUALS, Value = Wireless-802.11 (19)

It has been noticed that some organisations have applied filters to drop auth requests where the NAS-Port-Type (Attribute 61) does not match ‘Wireless-802.11’ (Value 19) and/or Service-Type (Attribute 6) does not match ‘Framed’ (Value 2). There is no requirement in the eduroam Tech Spec for such attributes to be forwarded, not least because some NASs do not send these attributes.

?**Peaks of re-authentications at certain times of the day/heavy auth load leading to failures and poor performance**

We use FreeRADIUS and AD and are experiencing issues at particular times of the day when our re-authentications appear to be increasing in frequency causing a large amount of failures. This is resulting in the eduroam(UK) Nagios check also being affected. What can we do to rectify this?

This is most likely to be due to slow responses from your AD when performing NTLM auth. It is a problem which affects all large institutions and there are different approaches to fix this. Some universities we have moved to using EAP-TLS as the primary authentication method, which doesn't require an AD auth. However, then you need a system to manage the client certificates. (E.g. Cloudpath ES but there are others.)

Some organisations, have moved to Samba 4 and tweaked the settings to improve performance. See the NWS 43 presentation on this subject.

Some quick fixes are to increase the MaxConcurrentApi setting on the Domain Controllers https://support.microsoft.com/en-us/kb/2688798 [24]

Where to find the authentication log files in FreeRADIUS 3 systems

Since different organisations configure their RADIUS servers in different ways, it is not possible to give a definitive answer as to where to find your log files. However, usually the log file will be in **/var/log/freeradius/radius.log**

The simplest configuration of FR 3 will utilise only one 'virtual FR' server for all auth flows. However, in 'advanced' deployments there may be dedicated virtual FR servers that handle auths for each of local users, remote roaming users and visitors. If so you may find that configuration of the logging is different in each virtual server. (These are virtual servers within FR, not actual virtual host machines).

Assuming a simple configuration, if you don't see the log file at /var/log/freeradius/radius.log you could look in /etc/freeradius/radiusd.conf (the FR config file) and find the section relating to logging, (log {) this is where the primary logging configuration for the FreeRADIUS server is located:

e.g.

```
log {
    destination = files
    file = ${logdir}/radius.log
#   requests = ${logdir}/radiusd-%{%{Virtual-Server}:-DEFAULT}-%Y%m%d.log
    syslog_facility = daemon
    stripped_names = no
    auth = no
    auth_badpass = no
    auth_goodpass = no
#   msg_goodpass = ""
```

```
#   msg_badpass = ""

}
```

The line file = ${logdir}/radius.log will indicate there the log files are.

Logs files are normally archived/rotated. In RedHat packaged implementations logrotate is responsible for rotating log files and you may find a logrotate file in /etc/logrotate.d/radiusd.

This /etc/logrotate.d/radiusd file is the configuration file specific to the radiusd service. Looking at that config file will show you the path of every RADIUS log file.

Now, whilst logging is normally carried out by writing to a log file as illustrated above, there are other methods.

Note the line destination = files in the config file. This destination for log messages need not be a file, it can be one of the following values:

files - log to "file" (as defined in the line just below)

syslog - send log messages to syslog (see the "syslog_facility =")

stdout - log to standard output (screen)

stderr - log to standard error

Note that the command-line debugging option "-X" overrides this option, and forces all logging to go to stdout.

6) eduroam(UK) Support Server / ORPS-related Questions

Do we need to give our ORPS a FQDN; can't we register the ORPS simply by its public IP address?

Yes it is an absolute requirement that you give the public IP address of your OPRS a FQDN; you cannot register an ORPS simply by public IP address. The eduroam(UK) Technical Specification https://community.jisc.ac.uk/library/network-and-technology-service-docs/eduroamuk-technical-specification-15 [25] states that our members' RADIUS servers must have a FQDN.

The reason for this is down to the design of the eduroam(UK) system in respect of the interaction between the Support Server and the NRPS. As the registration form is loaded, shared secrets for the ORPS-NRPS are generated. When the ORPS FQDN is entered, Support server does a DNS lookup and resolves the FQDN to an IP address. Registration of the new ORPS is completed when the [Save] button is hit. Then the IP address of the new RADIUS client/RADIUS authenticating server ORPS together with shared secrets are loaded into the NRPS configuration which is generated by Support Server. This is then uploaded to the NRPS at the next hourly refresh. It was originally decided (back in 2006) to engineer ORPS registration in this way, separating the ORPS entity from its IP address in the eduroam(UK) database to provide for our members to be free to change the IP address of their ORPS without needing to delete the peering in the system. Deleting the entity and subsequently re-creating a new one would result in the generation of new shared secrets and

require a configuration update (client and server config) on members RADIUS systems.

Making a change to the IP address of an ORPS

We are going to change the public IP address of our ORPS. Apart from changing our DNS entry is there anything we need to do in eduroam(UK) Support?

Yes. After changing the A/AAAA records in DNS, proceed with the following steps. Log in to Support server https://support.eduroam.uk. Click [26] on the Configure page. In the green 'RADIUS servers' panel, select your ORPS - this will result in a popup box appearing and the Support server will perform a DNS lookup. The IP address found should be your new IP address. Click on the [Save] button. The changes will be propagated to the NRPS at the next hourly config refresh (on the hour).

Note that the shared secret with the NRPS remains unaltered.

Since the public IP address of your ORPS is changing you will probably need to adjust the rules on your firewall.

IP address of ORPS displayed on Configuration page of eduroam(UK) Support server still shows old address some time after making the change in DNS.

Q. I changed the IP address of my ORPS server and updated DNS to reflect this yesterday, however the IP address displayed on the Configuration page on eduroam(UK) Support server still shows the old address, why is this?

A. This will be due to a too large TTL value associated with the record. E.g. a TTL of 172800 seconds applied to this record will mean it can be cached for up to 48 hours.

What category of RADIUS client to use for a server acting as proxy to the NRPS but not from the NRPS (to act as gateway to a 3rd party associate organisation)?

Q. "We are setting up a new RADIUS server to act as a proxy for the eduroam installations (at halls of residence) we are implementing with third parties. Instead of the new RADIUS server acting as a normal ORPS and therefore routing all the student authentications from the accommodation blocks via the NRPS (subjecting them to the heavy load which should be handled internally), we want to configure the accommodation block management company (acting as a 'Visited site') to use a local proxy server belonging to us so that we can forward local users to our RADIUS auth servers and filter out any junk auth requests before sending legitimate requests to the NRPS.

So how can we register our new RADIUS server on the Support website?"

A. 'Client only' is the setting to use. This results in the enabling of auth requests to be received by the NRPS, but no RADIUS packets will be sent to the RADIUS server you set as 'client only'.

How often is the sites information entered in the Support server uploaded to the eduroam locations map http://monitor.eduroam.org/gmap/country.php?country=uk [1]?

"The new sites/changed information about the eduroam service we provide at the site has not appeared on the eduroam map yet"

The UK sites location map is generated by eduroam Europe from information held in the European eduroam database. Sites data for eduroam(UK) participants *providing compliant operational services* is added to the European eduroam database by an automated script which polls the UK Support server (and all other federation members) every 4 hours. The data is made available to Europe via an XML file derived from the UK sites database. Then twice a day, the eduroam maps are generated through the build of KML files. Therefore it may take a while for a new site or updated data to appear on the eduroam maps after it has been added to the eduroam(UK) Support server, but it should never be more than a day before you see the changes.

7) eduroam Support Test System and Testing

We want to peer an ORPS with the NRPS and carry out tests without it becoming part of the production infrastructure and being sent production traffic, can this be accomplished?

Yes - see ORPS role designation features on Janet Roaming Support Server. In fact in order to facilitate testing, we have configured NRPS realm handling such that only traffic with your realm name prefixed with 'test' will be sent to your test/development server (see document).

Are there any test systems available to verify our system works/help with problem investigation? Where would I find these tests and are there any instructions on their use?

Yes - see section 12 on: Test Facilities on eduroam Support Server [27]

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

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

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

The eduroam test used to use anonymous@realm [28], however feedback from several organisations lead us to adopt the correct RFC format.

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

We're seeing a 'warning' issue detected on Support server: 'PEAP-MSCHAPv2 authentication failed: IPv4, RFC realm name'
What does this mean and how can we correct it? We have Microsoft NPS as our ORP

S.

The Support server test system has detected that your ORPS is rejecting users with anonymous outer userIDs. (Anonymous outer IDs such as [blank]@camford.ac.uk are permitted under RFC 4282).

NPS sites: To fix this you should edit your NPS connection request policies (for both your own roaming users and for visiting users):

- Enable "Override network policy authentication settings"
- Add in "Microsoft:Protected EAP (PEAP)"
- Untick the less secure authentication methods if any are enabled

Once you have applied these updates you can check that anonymous outer userIDs are being handled by running a 'roaming authentication test' via the Tests panel on your Troubleshoot page on Support server *having first ticked the 'RFC' box*.

The visitor simulation test is failing but the remote authentication test works for our site (indicating that shared secrets are fine). Why is this?

Our logs show 'remote server did not process authentication request'; packet sniffing shows that the ORPS keeps repeating the request and the eduroam test system repeats the challenge. Our firewall settings seem fine.

NRPS logs show 'incorrect login' authentication results, so the problem could be:

i) the wrong password is being used for the simulated visitor test; you must use the password you configured for the test user account on the eduroam Support server (not e.g. the password you use for login to your eduroam Support account)

ii) one of the shared secrets configured on your ORPS is incorrect - remember these are employed in both client and proxy areas of the ORPS configuration and are utilised independently; an error could mean that remote authentications are successful whilst visitor authentications fail.

Remote authentication tests from the eduroam Support web site fails but the simulated visitor test works. Why is this?

See above answer (ii)!

How can we test our implementation of CUI; does the simulated visitor test enable CUI to be tested?

The simulated visitor test supports the Chargeable User Identity (CUI) attribute and if your ORPS sends Operator-Name and CUI with the value 'nul' in the Access-Request, the Support server will return a CUI for that user in the Access-Accept.

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

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

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

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

Having just made changes to our config on the eduroam Support web site, errors are being recorded in our logs every five minutes - why?

Any changes to the test username/password and realm made on the eduroam Support web site are instantly put into the eduroam database. The on-demand tests on your test page on the eduroam web site are therefore instantly accessible.

There is however a background service availability monitor test powered by NAGIOS that is run from the eduroam Support server via one of the NRPS (usually roaming1). This runs a test authentication using the test account you have created in your user database and configured on the eduroam Support site. The NAGIOS probe configuration is however NOT updated/generated instantly and therefore there may a short period when test proble authentications fail and errors are logged on your ORPS. Once any config. changes have filtered through to the NAGIOS system, the test will run successfully and log error entires will cease.

What does the error condition 'HTTP CRITICAL - pattern not found' mean in the Nagios LG monitor for our site?

The web page, the URL for which you have registered in the Support server system, for your eduroam service information page doesn't have a link to http://www.eduroam.org [29] as is required in the eduroam(UK) Technical Specification. It is important for a number of reasons that users at all organisation participating in the federated eduroam service throughout Europe can easily find the parent eduroam confederation web site. It is a way of publicly asserting that your organisation is a member of the eduroam federation and subscribes to the federation policies. Nb. you are also required to exhibit the edroam logo on your service information web page.

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

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

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

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

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

If you have configured your OPRS into the Support server config page correctly, the above error is returned because you have set your ORPS as 'Test/Development'. This is resulting in preventing the NRPS from sending any auth traffic, including test traffic to you realm (only traffic with the 'test.' realm prefix will be sent). Refer to ORPS role designation features on JANET Roaming Support Server [30].

8) Upgrading FreeRADIUS from v 1.1.x to v2.0.x

Archive material - current version of FreeRADIUS is 3.0.x

Do you have any guidance for upgrading our system to FreeRADIUS v 2.0.x?

Whilst the upgrade to FreeRADIUS may at first seem daunting due to the change of structure and the new features, it is actually a very short task to migrate a live 1.1.x systems across to 2.0.x.

FreeRADIUS 2.0.x is a great improvement over 1.1.x and it is well worth making the effort to upgrade. 2.0.4 and upwards featured an 'inner-tunnel' method which means that eg EAP only hits your LDAP or SQL once...not the 3 or 4 times experienced previously. The current release is now 2.0.5 which has a lot of stats available via a simple query to the server and there will be new features going into 2.0.6 that will make it even more desirable, not least of which will be working SNMP and highly configurable logging capabilities.

Recommended approach to upgrading:

1) Examine the 1.x config to see what you have configured

2) Take the vanilla 2.0.x configuration and then edit it to add in the bits you did in 1.x this should be involve just the following:

a) edit sites-enabled/DEFAULT to match your authen/author/account fromt he old radiusd.conf

b) edit clients.conf and proxy.conf - exactly like 1.x initially

c) check out the other sites-available/* file to see what new functionality you want and then

enable those modules (eg inner-tunnel) by copying or softlinking them like the DEFAULT file entry (rename DEFAULT to 'university_of_foo' or whatever if you want)
- if you want to enable inner-tunnel, then edit eap.conf to use the inner-tunnel virtual server (highly recommended!)

d) after some local rad_check stuff, use the eduroam support server to ensure remote and home access is working.

We would then recommend setting up a proper proxy eduroam pool using the unlang (contact us for more advice etc on this aspect..some of it is covered on the support site FAQ)

9) Firewall Configuration

Why do I get only "Re-sending Access-Request" when testing authentication?

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

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

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

Why do we appear to not be getting any response from the eduroam NRPSs when visitors try to authenticate? Authentication requests are being sent from our ORPS but we get no response from the NRPSs. We have also tried authenticating with our eduroam test id ([our realm]@eduroam.ac.uk and [our_realm]@roaming.ja.net) and again get no response. This looks like a routing issue.

Troubleshooting - from the eduroam Support site tests:

a) the ping test shows that routing from the NRPS to your ORPS works and your ORPS responds

b) remote authetication tests PAP and the relevant EAP test results in success so your essential authentication system is correctly set up

c) since the problem is with outgoing authentication, this points towards a firewall configuration problem.

Problem resolution - whilst the firewall had been configured to allow incoming UDP 1812/13 from the NRPS to the ORPS and subsequent responses (ie outside authenication worked), there was no permission set to allow outgoing UDP to the NRPSs originating from the ORPS.

10) Wired Networks

How do you configure a Cisco Catalyst switch to operate with 802.1x?

Information on Cisco configuration can be found within the technical paper:

Configuring 802.1X Port-Based Authentication [31]

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/faqs-eduroam-system-administrators-and-implementation-techs-0

Links
[1] http://monitor.eduroam.org/gmap/country.php?country=uk
[2] http://www.techrepublic.com./article/ultimate-wireless-security-guide-self-signed-certificates-for-your-radius-server/
[3] http://support.microsoft.com/kb/814394
[4] http://www.ja.net/jcs
[5] https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations
[6] https://crt.sh/?id=1199354
[7] https://community.jisc.ac.uk/library/network-and-technology-service-docs/certificates-eduroam
[8] http://www.microsoft.com/downloads/details.aspx?familyid=1971D43C-D2D9-408D-BD97-139AFC60996B&displaylang=en
[9] http://www.novell.com/documentation/edir_radius/index.html
[10] http://wiki.freeradius.org/FreeRADIUS_Active_Directory_Integration_HOWTO
[11] https://social.technet.microsoft.com/Forums/windowsserver/en-US/e73183d4-7b2f-48a7-9246-97ed711e8e8d/eappeapmschapv2-realm-stripping?forum=winserverNAP
[12] mailto:userID@realm
[13] mailto:deviceID@realm
[14] mailto:device@camford.local
[15] mailto:device@realm
[16] mailto:service@ja.net
[17] https://support.roaming.ja.net/?q=general
[18] mailto:null@usersiterealmname.ac.uk
[19] mailto:anonymous@usersiterealmname.ac.uk
[20] mailto:realfred@usersiterealmname.ac.uk
[21] http://technet.microsoft.com/en-us/library/dd197475%28WS.10%29.aspx
[22] http://technet.microsoft.com/en-us/library/dd316177%28WS.10%29.aspx
[23] http://technet.microsoft.com/en-us/library/cc735393%28WS.10%29.aspx
[24] https://support.microsoft.com/en-us/kb/2688798
[25] https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcommunity.jisc.ac.uk%2Flibrary%2Fnetwork-and-technology-service-docs%2Feduroamuk-technical-specification-15&data=05%7C02%7Ceduroamuk%40jisc.ac.uk%7Caa52b8677f994ac4596208ddae5c7320%7C48f9394d8a
[26] https://support.eduroam.uk. Click
[27] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap
[28] mailto:anonymous@realm
[29] http://www.eduroam.org/
[30] https://community.jisc.ac.uk/library/janet-services-documentation/orps-role-designation-features-eduroamuk-support-server
[31] http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/Sw802