Published on *Jisc community* (https://community-stg.jisc.ac.uk)

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 24/05/2021

Contents

- 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.
- 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]?
- Making a change to the IP address of an ORPS

5) 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

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

- Guidance on upgrading to FreeRADIUS 2.0.x

7) 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?

8) Wired Networks

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

9) Wireless Networks

- How many SSIDs should be implement?
- Solving/mitigating the 'Overlapping eduroam Visitor service Problem' (aka the 'Russell Square' Problem)
- Do we have to support eduroam on 2.4GHz?

- Hints for Multi-floor Wi-Fi deployments
- Wi-Fi Surveying - help identifying a company which can provide a survey service
- Must we broadcast eduroam SSID rather than having it as a hidden SSID?
- Do we have to deploy a RADIUS server; can't we just peer our WLC with the NRPSs?
- How do you configure a Cisco 1200 Series Wireless Access Point for eduroam SSID?
- Can Cisco fat WAPs be used with multiple broadcast SSIDs and dynamic VLANs?
- Convertion of 'fat' Cisco WAPs into 'thin' ones
- WPA2 / WPA fallback for clients and APs - archived content

10) Supporting Users

- What sort of support for the users to we need to provide?
- How do I get access to the eduroam CAT (Configuration Assistance Tool) web site?
- What do I need to do to get my federated access SSO service to support my sys admin access to CAT?

1) Authentication Issues

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 [2]. '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 [3] (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 [3] 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. Such machines will not normally have RADIUS-routable usernames (since they will be in the form 'domain\hostdevice') and you must not try to create RADIUS-routable credentials for machines - although technically certificates could be issued in order to identify devices with a username 'device@realm [4]'.

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 issed 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

There are two cases when the NRPS don't respond to requests:

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 valid realm name.

2) eduroam Policy Related Issues and Dealing with Virus/Copyright Breach Incidents

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 [5] quoting 'eduroam' in the subject line. Contacts are listed on the eduroam Support Server General Information [6] 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 [5] 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 [7] or anonymous@usersiterealmname.ac.uk [8] or realfred@usersiterealmname.ac.uk

[9] 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 [6]

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).

3) <u>RADIUS Server log Keeping and interpreting Errors in the ORPS logs</u>

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 [10]

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. [11]

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. [12]

?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 [13]

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.

4) eduroam(UK) Support Server

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 beloinging 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'.

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 settings is there anything we need to do in eduroam(UK) Support?

No. Just change the DNS entry, the eduroam(UK) Support server will pick up the new IP and the NRPS will be reconfigured to use that when the configuration with the new IP gets pushed (on the hour).

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.

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.

5) 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 [14]

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 [15], 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 ORPS.

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 [16] 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 [17].

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

7) 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.

8) 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 [18]

9) Wireless Networks

How many SSIDs should be implement?

The answer to this is enitrely dependent on your needs and policy.

Obviously you'll need the eduroam SSID. By using dynamic VLAN assignment the one SSID can handle many groups of users and devices (e.g. staff, students, eduroam guests, other, 'machines'). This may meet the majority of your requirements.

Then you will probably want a setup/provisioning/remedial SSID (e.g. open, captive portal, access to installer utilities/CA certificate, OS patches)

In addition you may want an SSID for a non-eduroam guest service (e.g. for public access and either with a separate ISP feed or a tunnelled link through Janet to the contracted WISP service provider). But consider if eduroam Visitor Access could reduce the scale or need for expensive public access services.

If you have residences you may want an SSID for non-802.1X devices (e.g. multimedia devices, gaming, TV etc.).

http://www.revolutionwifi.net/revolutionwifi/p/ssid-overhead-calculator.html [19] useful for determining how many SSIDs you can handle. The old rule of thumb about no more than 4 SSIDs is based around broadcasting beacons at the old 802.11b 1Mbps rate. If you raise your minimum speed you can handle far more SSIDs with the trade-off of losing client connectivity at the margins. It could be argued that provision of a responsive service over a more limitied footprint (or one requiring a greater denisty of APs) is preferable to providing a poor data rate service that could lead to user dissatisfaction.

And you may need several SSIDs for WPA2-PSK services for specific purposes in specific limited locations. But consider implementing a single 'things' PSK wireless network.

How can we solve the overlapping eduroam service ('the Russell Square') problem? We would like to set up eduroam Wi-Fi but in a number of our buildings we get eduroam Wi-Fi from a neighbouring organisation. Some of our buildings are very close and the overlapping signal is very strong. We've been advised by our Wi-Fi supplier that any overlap would cause roaming issues for users. What are the possible solutions?

There are several solutions, however at the current time the best one is a technical method after political agreement (see below)

Technical method 1: use 802.11u (aka Hotspot 2.0/ HS20/passpoint) to identify the APs as being 'eduroam' but also belonging to your organisation. Compatible clients can then be configured to prefer the eduroam provided by your organisation. This is the ideal solution, however current client support is lacking (and when it is present it is fairly poor). The current eduroam position is decribed at:
https://wiki.geant.org/pages/viewpage.action?pageId=131634132 [20]

Technical method 2: conduct wireless surveys and liaise with your neighbouring organisation to ensure that wireless overlap is minimal, eg. turn down power of APs near the 'border zone' so that the correct APs are chosen by client devices when in the buildings in the overlap zone. This solution is complex and sometimes not possible due to wireless coverage patterns and required coverage areas from those bordering APs. This may also incurr additional cost due to the possible need to deploy additional APs to cover new dead spots and repositioning of APs.

Technical method 3 - don't provide the eduroam SSID where this service is provided through overlap from your neighbour - simply make use their eduroam wireless service in those areas. This obviously will mean that if you implement a single (eduroam) SSID network service with dynamic VLAN allocation for your own users, this will not be available at such locations. So you'll have a non-homogeneous/mixed service for your own users. Offsite (e.g. internet) resources will be accessible, but resources only available on a local user VLAN will be more difficult to access - although access could possibly be gained through a VPN. Visitors won't be affected, other than being unaware that the eduroam service they will be using will actually be being provided by your neighbour (potentially leading to support issues).

Political method - share layer2 VLANS between the 2 sites. You could feed your staff/student/visitor networks into each other's wireless domains and have RADIUS policy that states if the realm is that of your roaming L2 partner then allow agreed VLANs to be returned via their remote RADIUS server. For this to be viable you will need to have the transit mechanism, ie be neighbouring sites and connected to same NREN kit or have a direct link to your neighbour. This solution is the most satisfactory method for achieving inter-organisation roaming and ensures that when the staff/student/visitor client devices roam to the other location, they are still able to authenticate and drop onto the network as if they were on an AP in your own building.

This solution requires good, strong technical knowledge and the ability to share layer 2 networks between organisations (eg feed an 802.1Q trunk between sites). It needs to be done bilaterally (and can become very complicated when more than two organisations are involved) and with strict agreements/protection that you won't drop any other people onto such VLANS provided by you.

This is the preferred solution until hotspot2.0/802.11u becomes ubiquitous and method 1 becomes practicable (your wireless vendor's kit will need to support it and allow configuration of such beacon attributes).

Do we have to support eduroam on 2.4GHz?

No you do not have to support 2.4GHz eduroam. Indeed a 5GHz service could perform better in many situations. Have a look at the Optimize your WLANs for Phones and Tablets presentation (scroll to the near the bottom of the page) : https://www.jisc.ac.uk/events/wireless-mobility-event-27-feb-2019 [21]

For many organisations, for instance the NHS, where a lot of equipment is connected via Wi-Fi but much of the equipment only supports the 2.4G band, the case for providing eduroam in the 5G band (and future 6G band) is even stronger. This allows the 2.4G band to be dedicated to non-eduroam authenticated devices and avoids the need to advertise the eduroam SSID in the 2.4G band.

Do have any advice on Wi-Fi deployment for multi-floor buildings?

To improve handling of a multi-floor situation, consider rotating the antennas 90 degrees so they provide a smaller horizontal footprint but penetrate multiple floors more effectively, and then stagger APs between floors (if you are wanting a single eduroam instance to span the entire building), or you can dial down the power (or choose a cutting edge standard like 802.11ax that has less range) so that APs don’t penetrate between floors at all (this would even facilitate separate eduroam instances on different floors to support different departments for which for instance you might want to implement different filtering policies for staff/your own FE students/HE students).

Hint: Dialling down the power of APs is as important and dialling up the power to ensure coverage. You would dial down the power to a) match the power *from* laptops/phones since it is essential the AP can receive signals from devices and not simply shout at them! b) you need to ensure a clear transition boundary between the converage cells of adjacent APs to help devices to associate with specific APS without having to continually re-scan - which is time consuming for the device.

This presentation contains further hints and tips and is well worth a read: Optimise your WLANs for smartphones and tablets [22]

Wi-Fi Surveying - help identifying a company which can provide a survey service

Jisc (and before that Janet) has never offered a wireless network survey service to identify where signals are weak / strong across the campus buildings to help establish where additional access points may be required and to inform Wi-Fi network design. That is very much a campus network related service and not something that we as an inter-institutional / internet network provider have got involved in.

If your organisation does not wish to carry out the Wi-Fi surveying/review of design yourselves, wireless network surveying is very much the domain of commercial networking companies. To identify a suitable supplier, the Jisc purchasing frameworks programme might be helpful to your organisatoin. The frameworks programme is described on https://www.jisc.ac.uk/frameworks [23] and the specific one that might be useful is https://www.jisc.ac.uk/network-equipment-framework [24]. 'It also covers converged network adapters, interface modules, transceivers, access points, voice over internet protocol (VoIP) products and associated ancillary goods and services including software, cabling and installation.' There is a drop down menu listing the suppliers who are in the programme.

You may find the Network Equipment Framework – Buyer's guide of interest: https://community.jisc.ac.uk/system/files/56564/Network%20Equipment%20-%20Buyers%20Guide%20v.6.pdf [25] (you'll need to request membership of the Community group to access that).

Is it essential for an institution to broadcast the eduroam SSID, as opposed to having it hidden? And would failure to broadcast eduroam mean an institution couldn't join eduroam?

Yes to both questions. Broadcasting the eduroam SSID is required by eduroam confederation policy and is an eduroam technical requirement. This is because firstly, it's a way of advertising the presence of the service. Secondly, the native WinXP SP2 supplicant cannot do 802.1x against a hidden SSID (see below).

Do we have to deploy a RADIUS server; can't we just peer our WLC with the NRPSs?

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
6. Allow for upgrades/replacement of WLC separate from RADIUS service function

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

How do you configure a Cisco 1200 Series Wireless Access Point for eduroam SSID?

Details of the precise (largely web-based) steps used to configure the eduroam SSID on a Cisco® 1200 series WAP can be found in Appendix 2 of the case study Complying with the Janet eduroam Service Technical Specification.

Can Cisco fat WAPs be used with multiple broadcast SSIDs and dynamic VLANs?

There is a known problem with Cisco 'fat' WAPs with regard to multiple BSSIDs and dynamic VLAN assignment (RADIUS-assigned VLANs) which unfortunately affects a lot of institutions. The problem was that Cisco 'fat' IOS driven APs until recently only supported a single primary (guest) SSID broadcast in the beacons (the BSSID). Furthermore, it was not possible to achieve assignment of VLANs via RADIUS. This limitation does not apply to Cisco's 'thin' architecture, so the problem could hitherto only be circumvented by adopting this technology.

This issue only affected the autonomous Cisco APs. There never was any difficulty with lightweight APs (including upgraded autonomous ones) in supporting RADIUS-assigned VLANs and multiple broadcast SSIDs. (Certainly 1131 and 1232 APs in non-autonomous LWAPP thin client mode with WiSM controllers have always worked fine).

With release 12.3.8-JEC(GD) of the Cisco IOS firmware, this issue has been resolved - certainly multiple BSSIDs with RADIUS assigned VLANs have been successfully setup with AP1231 and other 1200 series access points.

Although the issue has been resolved in the IOS, you may find that some AP radios do not support multiple BSSIDs. To find out if a particular radio will support multiple BSSIDs:

Run a 'show controllers' *radio_interface* command to check how many BSSIDs an AP will support. Look for the line which states - "Number of supported simultaneous BSSID on Dot11Radio0: 8", or something similar.

To set up multiple BSSIDs on the AP you can log into the web interface and select Security > SSID Manager. The page displayed will show the current VLANs configured and indicate which are being broadcast.

Alternatively from the IOS command line, enter SSID configuration interface and use the command mbssid. You'll also have to use mbssid from the configuration terminal interface to enable multiple basic SSIDs on an access point radio interface. This command was introduced in IOS release 12.3(4)JA.

See: Cisco IOS mbssid command [26]

[NB. The validity of following advice with regard to latest release of IOS is unknown - it certainly applied to pre-12.3.8 releases]. The Cisco WAP beacon can by default advertise only one broadcast SSID, nevertheless it is possible to alert client devices of additional SSIDs although this did not remove the limitation that RADIUS-assignment of VLAN was not possible. You can achieve client alerting of multiple SSIDs as follows; use the SSID list information elements (SSIDL IEs) in the access point beacon to alert client devices of additional SSIDs on the access point. When you designate an SSID to be included in an SSIDL IE, client devices detect that the SSID is available, and they also detect the security settings required to associate using that SSID.

See: Cisco AP Configuration Guide - Configuring Multiple SSIDs [27].

The AP configuration needs to use the command: information-element ssidl [advertisement] [wps](Microsoft Wireless Provisioning Services) [28] in the radio interface configuration / specific SSID configuration section.

For WinXP users the following download must be installed. This update enhances Windows XP support for Wi-Fi Protected Access 2 (WPA2) options in Wireless Group Policy (WGP), and helps prevent the Windows wireless client from advertising the wireless networks in its preferred networks list.

WinXP Update:

- http://www.microsoft.com/downloads/details.aspx?familyid=2726F32F-D52B-4F84-ACE8-F7FC20195769&displaylang=en [29]!!!
- http://support.microsoft.com/kb/917021 [30]

Using this update, the 'hidden' SSIDs become visible in a Cisco 'fat' AP environment - the subsequent SSIDs use the extension made available through 802.11i.

Can you expand on what is necessary to convert 'fat' Cisco WAPs into 'thin' ones? (Is it just an IOS upgrade and does it cost anything? What device(s) do you use to control them? Do you lose any functionality in converting to thin?)

Changing to thin is a straightforward job. Either use the IOS command line (archive download-sw tftp://.........), the windows-based upgrade tool [31] or a WLSE (Wireless LAN Solution Engine). The upgrade tool and software image can be downloaded free from Cisco [31], and the tool pushes the image to the APs you tell it to, which converts them to lightweight. They then get their configuration from the controller rather than it being stored locally.

To control these thin APs you need a central controller, which incurs a cost. Lightweight wireless means all the clever stuff (authentication, key management, channel and power management) is done by a central box. This could be the Wireless Services Module (WiSM) for the Cisco Catalyst 6500 switch

[32] (controls upto 300 APs), the standalone Wireless Control System (WCS) [33] or the Catalyst 3750G Integrated Wireless LAN Controller [34] (can only control about 32 APs). There's a fair amount of configuration to do so the controller knows about your VLANs, SSIDs, RADIUS servers etc.

You gain a great deal of functionality and management facilities - such as reporting, accounting, configuring WLANs, mobility etc. You manage the APs bia a web interface on either the controller or a PC running Cisco's WCS software, which co-ordinates multiple controllers and does RF planning etc. Adding a new access point is a straightfoward task of connecting it to a switch and then using the software to put the switch port in the right VLAN.

Summary:

- WAPs must have IOS 12.3(7)JA or higher
- Thin IOS must then be loaded via WinXP program (available on Cisco web) or via CLI
- The WAPs must be 1240AG/1130AG/1200 series [1210,1220,1230,1235]
- (1200 series radios must be one of following models only: MP21G/MP31G/RM21A/RM22A)
- Wireless controller module (WiSM) of some description necessary [WiSM for Catalyst 6500 (will need a free slot), WCS or Catalyst 3750G IWLC]
- Catalyst 6500 requirements: free slot for WiSM, Supervisor Engine 720 [35] WS-SUP720 needed and to run a SUP720 you need the higher rated PSU
- For large deployments of three or more WiSM, a WCS is recommended

There is a guide to the process on the Cisco web site: Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode [36]

To get the upgrade tool and Cisco IOS release:

- Browse to the wireless downloads page: http://www.cisco.com/en/US/products/hw/wireless/index.html [37]
- Click Access Points.
- Click the type of access point that you want to upgrade. When you click the access point type, the access point folder expands.
- Click the access point that you want to upgrade in the expanded list. The Select a Software Type list appears.
- For the upgrade tool, click the Autonomous to Lightweight Mode Upgrade Tool link.
- For the software image, click the Autonomous to Lightweight Mode Upgrade Image link.

Will a client configured for WPA2 fallback to WPA in a WPA-only environment?

Solving/mitirating the Overlapping eduroam Visitor service Problem (the 'Russell Square' Problem)

The overlapping eduroam service scenario is a well-known issue in eduroam. In the UK the way to address this is for organisations sharing the same locale to talk to each other and co-operate to minimise the overlapping Wi-Fi zones. This can be achieved by careful positioning of APs, reducing radio power and using non-omnidirectional antennae.

Other solutions require even closer co-operation and involve partial integration of networks (for instance the bigger organisation could provide Wi-Fi service across both campuses, providing an eduroam Visited service for both, and establish local RADIUS peering with the co-located organisation).

Archive Questions:

Will an AP configured for WPA2 fallback to WPA if a WPA-only client tries to associate?

The native Windows XP supplicant software requires the user to make an explicit choice between WPA and WPA2 when performing the configuration. If a user with a device configured for WPA2 visits a site where the guest WLAN has been configured to utilise WPA, will they be denied service, or does the client fall back to WPA? Similarly if the guest WLAN has been configured for WPA2 and a visitor arrives with a device configured for WPA will the APs fall back to support WAP or will the user experience problems?

It will probably be the case that a client set up to use WPA2 will not work at a WPA location - this depends on the supplicant and the configuration. Generally a client needs to have the correct specific cipher methods configured. Likewise a client configured to use WPA will not work in a WPA2-only location.

Some clients can handle both WPA and WPA2 versions of the same SSID... and some clients (eg Vista) can even have different profiles pointing to the same SSID. See Workstation/Laptop Setup [38] above.

However, since the vast majority of clients only support WPA at present, we advise that JRS3 WPA2 sites should still provide WPA connectivity and JRS2 sites must provide WPA (and they may also provide WPA2). This advice will stand until we see a wholesale migration to WPA2 (which is expected in a few years time).

Our Cisco 1200 autonomous-mode APs have been configured using the 'cipher' option of 'AES CCMP + TKIP'. Does this mean that our WLAN is effectively supporting both?

Yes, it should support both - you can determine this by using a wireless card or probe that tells you what ciphers it can detect, eg. the 'airport' utility in MacOSX.

We recommend that the cipher mix is kept to the standards - eg WPA/TKIP and WPA2/AES.- Whilst WPA/AES exists it is very exotic and WPA2/TKIP is just wrong.

Another reason to implement WPA2/AES (alongside WPA/TKIP) is that only with AES can true 802.11n speeds be obtained (apart from in a wide open wi-fi scenario) - so anyone looking at 802.11n kit needs to keep this in mind.

Useful links:

- Wireless assistance\\Tech Guide: Wi-Fi: Security For The Masses [39]
- 802.1X Port Access Control for WLANs [40]
- Deploying 802.1X for WLANs: EAP Types [41]
- Wireless on Linux, Part 1 [42] and Part 2 [43]
- Open1X.org - Selecting An Appropriate EAP Method For Your Wireless LAN Evolution of WLAN Security [44]

10) Supporting Users

What sort of support for users to we need to provide?

We would expect organisations providing eduroam services to provide their users with adequate support; as a minimum, in addition to the organisation's eduroam service information web pages which must provide help on how to use eduroam and device set up instructions, the organisation's IT helpdesk should have the capability to:

- provide guidance on the set up of users' devices for operation with eduroam
- check the status of a user's account to ensure that they are eligible to use eduroam
- check RADIUS logs to see if authentication requests are being received for the user's authenitcation attempts and the outcome of those attempts

PS We have published a supporting users troubleshooting flowchart, designed for help desks which may be of some help:
eduroam-users-troubleshooting-flowchart-it-support-staff.pdf [45]

How do I get access to the eduroam CAT (Configuration Assistance Tool) web site?

To use the eduroam CAT tool (developed through the Geant eduroam confederation), you need to have a compliant Home service and an invite token. To get a invite token go to your eduroam(UK) Support server main configuration page and click on the eduroam CAT invite button. A token will be sent **to the e-mail address you have registered as the primary technical contact** on the web site. **The token expires after 24 hours**, so must be used before then. (Nb. If you have only just changed your compliance assertion on eduroam(UK) Support server you will have to wait until the update replicates through to the European database for your organisation to be listed on CAT).

For more information see eduroam CAT [46].

What do I need to do to get my federated access SSO service to support my sys admin access to CAT?

Your federated access SSO IdP needs to release eduPersonPrincipalName and eduPersonTargetedID attributes to the https://monitor.eduroam.org/sp/module.php/saml/sp/metadata.php/default-sp [47] SP. It may be the case that your IdP will release these without any further configuration or you may find that your IdP needs to be modified.

Create policy for cat.eduroam.org attribute release

The **attribute-filter.xml** file needs to have this policy in place before your sign on will function

```
<afp:AttributeFilterPolicy>
<afp:PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="
<afp:AttributeRule attributeID="eduPersonPrincipalName">
<afp:PermitValueRule xsi:type="basic:ANY" />
</afp:AttributeRule>
<afp:AttributeRule attributeID="eduPersonTargetedID">
<afp:PermitValueRule xsi:type="basic:ANY" />
</afp:AttributeRule>
<afp:AttributeRule attributeID="cn">
<afp:PermitValueRule xsi:type="basic:ANY" />
</afp:AttributeRule>
```

```
<afp:AttributeRule attributeID="mail">
<afp:PermitValueRule xsi:type="basic:ANY" />
</afp:AttributeRule></afp:AttributeFilterPolicy>
```

Source URL: https://community-stg.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] mailto:userID@realm
[3] mailto:deviceID@realm
[4] mailto:device@realm
[5] mailto:service@ja.net
[6] https://support.roaming.ja.net/?q=general
[7] mailto:null@usersiterealmname.ac.uk
[8] mailto:anonymous@usersiterealmname.ac.uk
[9] mailto:realfred@usersiterealmname.ac.uk
[10] http://technet.microsoft.com/en-us/library/dd197475%28WS.10%29.aspx
[11] http://technet.microsoft.com/en-us/library/dd316177%28WS.10%29.aspx
[12] http://technet.microsoft.com/en-us/library/cc735393%28WS.10%29.aspx
[13] https://support.microsoft.com/en-us/kb/2688798
[14] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap
[15] mailto:anonymous@realm
[16] http://www.eduroam.org/
[17] https://community.jisc.ac.uk/library/janet-services-documentation/orps-role-designation-features-eduroamuk-support-server
[18] http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/Sw802
[19] http://www.revolutionwifi.net/revolutionwifi/p/ssid-overhead-calculator.html
[20] https://wiki.geant.org/pages/viewpage.action?pageId=131634132
[21] https://www.jisc.ac.uk/events/wireless-mobility-event-27-feb-2019
[22] http://optimise-your-wlans-for-phones-and-tablets
[23] https://www.jisc.ac.uk/frameworks
[24] https://www.jisc.ac.uk/network-equipment-framework
[25] https://community.jisc.ac.uk/system/files/56564/Network%20Equipment%20-%20Buyers%20Guide%20v.6.pdf
[26] http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/command/reference/cr12410b-chap2.html#wp2700587
[27] http://www.cisco.com/en/US/docs/wireless/access_point/12.3_7_JA/configuration/guide/s37ssid.html#wpxref78332
[28] http://www.microsoft.com/technet/community/columns/cableguy/cg1203.mspx
[29] http://www.microsoft.com/downloads/details.aspx?familyid=2726F32F-D52B-4F84-ACE8-F7FC20195769&amp;displaylang=en
[30] http://support.microsoft.com/kb/917021
[31] http://www.ja.net/services/authentication-and-authorisation/janet-roaming/technology.html#cisco_AP_thin_upgrade_tool
[32] http://www.cisco.com/en/US/products/ps6526/index.html
[33] http://www.cisco.com/en/US/products/ps6305/index.html
[34] http://www.cisco.com/en/US/products/ps6915/index.html
[35] http://www.cisco.com/en/US/products/hw/modules/ps2797/ps5138/index.html
[36] http://www.cisco.com/en/US/products/hw/wireless/ps430/
[37] http://www.cisco.com/en/US/products/hw/wireless/index.html
[38] http://www.ja.net/services/authentication-and-authorisation/janet-roaming/technology.html#multiple_encryption_profile_Vista
[39] http://www.informationweek.com/story/showArticle.jhtml?articleID=10808186
[40] http://www.wi-fiplanet.com/tutorials/article.php/3073201

[41] http://www.wi-fiplanet.com/tutorials/article.php/3075481
[42] http://www.wi-fiplanet.com/tutorials/article.php/3066371
[43] http://www.wi-fiplanet.com/tutorials/article.php/3081601
[44] http://open1x.sourceforge.net/links.html
[45]
https://jisc365.sharepoint.com/:b:/s/PublicDocumentLinks/EZDTqQ6rTGVFn0p_xquaAJQBAjUKSPXggAll5lqj5JjTHA
[46] https://cat.eduroam.org/
[47] https://monitor.eduroam.org/sp/module.php/saml/sp/metadata.php/default-sp