# OpenRoaming requirements checklist

Here's a requirements checklist to use when you want to deploy OpenRoaming (or when you are trialling [1] it):

## 1. Check your Wi-Fi infrastructure

Your Wi-Fi infrastructure must be Hotspot 2.0 compatible. This means it has to support ANQP (802.11u), ideally WPA3-Enterprise (although WPA2-Enterprise is sufficient), and has to have functionality available to support Passpoint Release 1 or 2 (3 includes the previous two) in the settings to be able to set Roaming Consortium OIs (RCOIs), Operator names and the like. If you have already deployed a WPA3-Enterprise network, do not switch 192-bit security on for WPA3. It is not compatible with OpenRoaming. You are required to use Protected Management Frames (PMF).

Most recent enterprise-class kit from Aruba, Ubiquiti, Meraki and Cisco should support all of the above. If your kit datasheet or technical details mention Passpoint R1, R2, or R3, then you should be set. OpenWRT-powered kit does support Hotspot 2.0 to a degree. If you are unsure, please ask the vendor to confirm which of their devices support Hotspot 2.0 or Passpoint.

If you use web-managed devices, like Meraki's MR series, you may need to ask your vendor's tech support to either show you where the Hotspot 2.0 settings are or, if they don't seem to exist, enable them for you. On Aruba Instant APs or standalone APs running the latest version of ArubaOS 8 (both of which have their own built-in UI), you are required use the command-line, or you can export your configuration, modify the configuration in a text editor, and then import that modified configuration to enable OpenRoaming.

## 2. Check your RADIUS server

Your RADIUS server should support Radsec. OpenRoaming uses Radsec to shuttle traffic around the world. When a user visits an Access Network Provider (ANP - similar to a visited site in eduroam land), the ANP's RADIUS server will dynamically look up where to send the user's request. The ANP server then connects directly to the user's home service via Radsec to securely complete the authentication.

OSC Radiator does (and does dynamic discovery very well), FreeRADIUS does (but we have not tested dynamic discovery), radsecproxy also does (and does dynamic discovery well). Cisco's ISE and Aruba's Clearpass Policy Manager also support Radsec, but we have not tried to see if either support dynamic discovery or not.

Unfortunately, Microsoft NPS does *not* support Radsec, but by pointing it at a Radsecproxy instance (either running in the Linux subsystem for Windows or on a dedicated VM or Docker container for dynamic routing, or directly in Windows for static routing), you ought to be able to

support OpenRoaming.

Additionally, if using Microsoft NPS as your server, you ***must*** add the user 'anonymous' into your Active Directory instance, but you can disable it (it merely needs to exist). Recent versions of Android will use the user 'anonymous' as the so-called outer identity for OpenRoaming, and if the user does not exist, the authentications will fail!

**Note:** If you use our OpenRoaming proxy service (which you would for our trial), we continue to support UDP over port 1812, but just like with your eduroam servers, we need to register these in our configuration. If you are using eduPKI certificates [2] with Radsec to connect to our eduroam national roaming servers, you can also use these with our OpenRoaming proxy service.

## 3. Check your DNS server

Your DNS server software (or DNS service) must support NAPTR records. NAPTR records are often used for SIP services, but eduroam uses NAPTR records to indicate to other countries' roaming operators where to send traffic, which is faster than sending it one hop at a time up and along a server chain. OpenRoaming, being a mesh-like roaming federation, does exactly the same.

We know that there are well-known DNS services out there that notably do *not* support NAPTR records. Azure is currently one of them (although we understand that Microsoft is working to add NAPTR support to Azure DNS). The Jisc Name Server service [3]does support NAPTR records, as do Cloudflare [4] and Infoblox [5]. Linux server software like BIND, and Windows DNS server do too. Please let us know if you use software on other platforms that support (or don't support) NAPTR records.

To check that your NAPTR record is correctly configured, use the NAPTR Lookup [6] at DNS Lookup Online and stick your realm name in.

## 4. Consider your network options

**Do you just want to provide your users with the ability to roam onto OpenRoaming networks (i.e. just act as an identity provider)?**

- If so, then as an existing eduroam member you do not need to do that much. **Note:** We're still working through the details of what is required for identity providers, but the basics are the same between eduroam and OpenRoaming.
- You must set up a NAPTR record in your DNS records to point to our OpenRoaming proxy. The NAPTR record is similar to the existing record we require for non-.uk domains (so .org, .net and .com). This NAPTR record will tell any ANPs where to route your traffic (to us). We'll do the rest, and you ought to see OpenRoaming requests flow to you via our existing eduroam proxies. Details of the NAPTR record are further down in the **Technical information** section.
- If you are using geteduroam (eduroam CAT), you must add some options into your existing profile, or create a new profile specifically for OpenRoaming (which will automatically also include eduroam).

**Do you want to provide OpenRoaming visitors with the ability to roam onto your network (i.e. act as an ANP)?**

- If you are currently receiving Internet from Jisc via the JANET network, you must ensure that any non-educational OpenRoaming traffic does not exit through the JANET network (note: **this only applies to traffic after authentication**). This means getting a broadband connection from another telecomms supplier in order to segregate education traffic from non-education traffic (if you already have a guest network solution like The Cloud, BTOpenZone or similar, you will already have such a connection).
- You should also ensure that your visiting eduroam users and your OpenRoaming users are not on the same VLAN. OpenRoaming provides specific beacon values (see further below) to indicate whether educational users, mobile users that just want free Internet, or users who will pay for their Internet, can connect to your network, so you can provide specific Hotspot 2.0 VLANS and SSIDs that segregate these. A VLAN with client isolation is probably the best option.
- Contact us [7] for a secret for our OpenRoaming proxy (details are in the **Technical information** section below), which we keep separate from our eduroam national roaming servers for engineering reasons. Effectively, we will do the hard work of routing the OpenRoaming traffic for you. If you are one of the few eduroam members who connect to our roaming servers with Radsec, you can also use Radsec with the OpenRoaming proxy to secure your outgoing authentication traffic.

**Do you want to be able to provide both your users with the ability to roam *and* allow OpenRoaming visitors onto your network (i.e. act as both an identity provider *and* as an ANP)?**

- Simply combine the two sets of requirements above.

## 5. Setting up your network (as an ANP/Visited Organisation)

Supposing that you have enterprise-class access points that you can configure for Hotspot 2.0/Passpoint R1-3, you will need RCOI values to indicate what kind of network you are providing. The ANQP beacon features in access points only broadcast three RCOI values, and you can provide an additional three values by ANQP query.

For an OpenRoaming network that is for eduroam or educational users only, use one or more of the following RCOIs:

001BC50460 (eduroam)
001BC5046F (eduroam)
5A03BA1900
5A03BA3900

For an OpenRoaming network that is for any identity, use one or more of the following RCOIs:

5A03BA0000
5A03BA0800
5A03BA1000
5A03BA1800

5A03BA2000
5A03BA2800

To include the eduroam RCOI and the educational RCOIs, simply combine values from both lists.

We would recommend broadcasting these three values:

001BC50460 (eduroam)
5A03BA0000 (the WBA RCOI for free OpenRoaming)
004096 (Cisco's 'legacy' RCOI for OpenRoaming)

The WBA makes available a handy RCOI calculator here: https://wireless-broadband-alliance.github.io/OR-rcoi-config/ [8]

## 6. Setting up your network (as an IDP/Home Organisation)

To enable OpenRoaming in your CAT profile, open your CAT profile in the CAT admin interface.

Then, in the **Media Properties for this profile** section, add the **OpenRoaming** option and choose the appropriate option for your organisation:

- **Ask User** will prompt the user whether they'd like to add OpenRoaming.
- **Ask User, T&C pre-agreed** will pre-agree the Wireless Broadband Alliance Terms and Conditions
- **Always** and **Always, T&C pre-agreed** will be the inverse, opting to add OpenRoaming by default

The default profile options will install the eduroam RCOI (001BC50460) by default. To add additional RCOIs, use the **Media Properties for this profile** section again, but choose the **Additional HS20 Consortium OI** option. We recommend adding these additional values:

- 5A03BA0000 (the Wireless Broadband Alliance RCOI for free OpenRoaming)
- 004096 (Cisco's 'legacy' RCOI for OpenRoaming)

The WBA makes available a handy RCOI calculator here: https://wireless-broadband-alliance.github.io/OR-rcoi-config/ [8]

## 7. Testing your network (as an ANP/Visited Organisation)

To test your network, you can use the 'eduroam.ac.uk' test identity we make available in the eduroam Support portal Troubleshoot page. To use it, download the geteduroam app onto a mobile device, select the 'Camford University' organisation, and then choose either the 'eduroam plus edu RCOI' or the 'eduroam plus settlement-free RCOI' profiles. Use your 'eduroam.ac.uk' test credentials there.

On your device, change the option in the 'eduroam' network settings to not automatically connect, disconnect from the eduroam network and wait for your device to interrogate the beacons before it then attempts to connect to your OpenRoaming network SSID.

Assuming that your access point beacons allow *all* of the above beacon values, you should see the following behaviour:

- On a geteduroam-configured mobile phone, you may see the realm of your identity (if you use our eduroam.ac.uk test identity, it will show eduroam.ac.uk), followed by the words 'via Passpoint'. This is the eduroam credential configured to connect to OpenRoaming.
- On Samsung Galaxy S-series (and some A-series) phones specifically, you will likely see an 'OpenRoaming' network without you having done anything. This is expected because on these devices, Samsung automatically enrolls you into OpenRoaming with your Samsung identity. We find that the connectivity can be spotty (i.e. you must retry several times before it connects).
- On Google Pixel phones, Google also makes the OpenRoaming network available. When tapped to connect for the first time, the network entry will prompt you for terms and conditions, after which it will connect using your Google identity. This may also be spotty, but it is generally more stable than Samsung.
- You also have the ability to use some other apps, such as Cisco OpenRoaming (Google Play [9], Apple App Store [10]) or GlobalReach's GlobalRo.am (Google Play [11], Apple App Store [12]). In these apps, you can sign in with either your Google or your Apple identity, and the phone should connect to your OpenRoaming network.

## 8. Testing your network (as an IDP/Home Organisation)

To test your profile, download the geteduroam app onto a mobile device, select your profile, and then use your own credentials there.

On the device, change the option in the 'eduroam' network settings to not automatically connect. If you have an OpenRoaming network, disconnect from the eduroam network and wait for your device to interrogate the beacons before it then attempts to connect to your OpenRoaming network SSID.

If you do not have an OpenRoaming network, check the Global OpenRoaming Locations [13] map for the nearest hotspot to try. In the UK, we can confirm that Loughborough, Coventry, Oxford, and Bristol all have functional hotspots, while greater London has a lot of access points. Olympic Park, Elephant & Castle, Holborn and some South London locations host hotspots from Loughborough University and the University of Arts London. The City of Westminster is rolling out OpenRoaming into various public buildings as part of the Connected London initiative.

## 9. Advertising your locations (as an ANP/Visited Organisation)

Advertise your OpenRoaming locations by telling us where you have rolled out OpenRoaming (even if just as a trial), so that others wishing to test their own OpenRoaming trial implementations in the area will have an easy place to try and test their off-campus roaming ability. The Wireless Broadband Alliance (WBA) are also interested in knowing where OpenRoaming is being used, and they are collating locations to publish to their membership.

Currently the most well-known **functional** locations in the UK are Loughborough University in both Loughborough itself and in Olympic Park in east London, the 22 Bishopsgate office

building in the City of London, and University of the Arts London campuses across South London and Holborn. The City of Westminster are rolling out networks across their area of London. Two locations in the Oxford area and in Bristol are also functional.

There are larger deployments elsewhere in Europe (notably the Delhaize Supermarket group deployed OpenRoaming to all its supermarkets in Belgium and Luxembourg), Asia (the Japanese cityroam network spans much of the Japanese main islands) and the US.

Inspired and spurred on by some of our early work, the Wireless Broadband Alliance now publishes a 'live' map (updated every 24 hours based on beacon advertisement), similar to the eduroam map available through the eduroam Companion app, here: Global OpenRoaming Locations [13]

## Technical information for our service

### NAPTR Record

To use our service, you must insert this NAPTR record into your DNS configuration:

| Type | Order | Preference | Flags | Services | Regexp | Replacement |
|---|---|---|---|---|---|---|
| NAPTR | 100 | 10 | s | aaa+auth:radius.tls.tcp | | _radsec._tcp.openroam |

You can add multiple records with different preferences if you also would like to add the European eduroam OpenRoaming proxy as a backup service. In their case, replace the '**.uk**' in the 'Replacement' segment with '**.org**'.

### Proxy server address

We use two different hostnames for our proxy server:

- For connecting via UDP/1812, use **openroaming0.eduroam.uk**. In this case, contact us [14] and we'll register your server as a client and issue you with a secret.
- For connecting via TCP/2083 (Radsec) with eduPKI (eduroam-issued Radsec) certificates, use **openroaming0e.eduroam.uk**
- For connecting via TCP/2083 (Radsec) with WBA (or one of their agents) certificates, use **openroaming0.eduroam.uk**

If you prefer IP addresses over hostnames, use IP addresses as follows:

- openroaming0.eduroam.uk: 193.63.195.37 (IPv4), 2001:630:1:132::37 (IPv6)
- openroaming0e.eduroam.uk: 193.63.195.38 (IPv4), 2001:630:1:132::38 (IPv6)

### Operator-Name attribute

On FreeRADIUS, Cisco ISE, Aruba Clearpass Policy Manager, Packetfence and Radiator, you can specify a value for the Operator-Name attribute. In eduroam, the value is '**1your-realm.ac.uk**'. In OpenRoaming, when sending OpenRoaming traffic, you should now use '**4<WBA ID>**' where WBA ID is an identifier issued or registered with the WBA. The European

eduroam proxy's WBA ID is '**4EDUROAM**', while ours is '**4JISC:GB**'.

Please use '**4YOUR-REALM.EDUROAM.JISC:GB**' for your outgoing OpenRoaming traffic via our proxy, where YOUR-REALM is the value in the 'Identifier' box on the eduroam Support portal (on the Configure page in the 'Organisation settings' box), but without the '.AC.UK' suffix. For example, Camford University would use '4CAMFORD.EDUROAM.JISC:GB' as the correct value. If you can't set an Operator-Name attribute on your side, we will set it automatically in line with the existing eduroam Support portal behaviour.

On incoming traffic from our eduroam NRPSes, you can distinguish OpenRoaming traffic from normal eduroam traffic by looking at the Operator-Name attribute. Anything coming from the European OpenRoaming proxy will be labelled '**4EDUROAM**', while anything from our OpenRoaming proxy will be labelled '**4JISC:GB**' or a value ending with '**JISC:GB**'. If you happen to roam onto an OpenRoaming network elsewhere in the world with your test device, you should see '**4<their WBA ID>**', e.g. when roaming in Japan, you would most likely see '**4CITYROAM**'.

## Troubleshooting your OpenRoaming network

Troubleshooting OpenRoaming can be, when this is brand-new to you, more protracted than it should be. For the most part, OpenRoaming is just like eduroam, so the same basic rules apply, such as ensuring that your firewall allows RADIUS UDP traffic from your servers to exit your organisation, and vice versa.

Test an EAP authentication using eapol_test (or eapol_test.exe, on Windows) and an appropriate credential (such as the eduroam.ac.uk credential available for troubleshooting eduroam) from a device connected to your network. A sample test configuration (save it as a text file with any file extension you like) looks like this:

```
network={
phase1="tls_disable_tlsv1_0=1 tls_disable_tlsv1_1=1
tls_disable_tlsv1_2=0 tls_disable_tlsv1_3=1 peapver=0"
key_mgmt=WPA-EAP
eap=PEAP
identity="<username@realm>"
anonymous_identity="<username@realm>"
password="<userpassword>"
phase2="eapauth=MSCHAPV2 mschapv2_retry=0"
}
```

Note: Be careful with the above quotation marks (some modern text editors will turn them into "smart quotes").

Replace the identity and anonymous_identity items in the configuration above with the eduroam.ac.uk credential, and insert the password. Then save the file. Then use it with the eapol_test binary (on Linux) or executable (on Windows) as follows:

```
eapol_test -c <your config file> -a <IP address> -s <secret>
```

If running this on your RADIUS server, you should use the IP address of the OpenRoaming proxy and the secret we provided you with for your server in the appropriate spots above. If running this from a mobile device on your network, this may be routed through your default gateway instead (in which case, please let us know what your default gateway is).

A successful EAP authentication will result in a lot of fast-scrolling text and an eventual 'SUCCESS' message. A failure with a TIMEOUT will mean that something stopped the traffic to get to us (or our return traffic to be returned to you), or your packets were possibly ignored on our proxy (in which case, we'll check and then ask you to try again).

A successful test should then lead on to successful authentications with any device configured with OpenRoaming.

## More information on eduroam and OpenRoaming

Our colleagues in the European eduroam infrastructure team have extended notes on Passpoint networks (which includes OpenRoaming). You can see these here:

Roaming on Passpoint-based network infrastructure (incl. OpenRoaming) [15]

## More advanced topics

Joining OpenRoaming on your own (we're working on some check lists and process flows with the WBA for this, please bear with us).

Joining the WBA on your own (we're working on some check lists and process flows with the WBA for this, please bear with us).

---



**Links**
[1] https://community.jisc.ac.uk/library/network-and-technology-service-docs/call-partipation-openroaming-collaborative-investigation
[2] https://eduroam.org/support/edupki-eduroam-ra/
[3] https://beta.jisc.ac.uk/primary-nameserver-service
[4] https://blog.cloudflare.com/additional-record-types-available-with-cloudflare-dns/
[5] https://docs.infoblox.com/space/nios86/36637408/NAPTR+Record
[6] https://dnslookup.online/naptr.html
[7] mailto:eduroamuk@jisc.ac.uk?subject=eduroam%20UK%20OpenRoaming%20Proxy
[8] https://wireless-broadband-alliance.github.io/OR-rcoi-config/
[9] https://play.google.com/store/apps/details?id=com.cisco.or
[10] https://apps.apple.com/gb/app/openroaming/id1496830649
[11] https://play.google.com/store/apps/details?id=com.grtconnect
[12] https://apps.apple.com/gb/app/globalro-am/id6447584451
[13] https://wballiance.com/openroamingmaps/
[14] mailto:eduroamuk@jisc.ac.uk?subject=Registering%20an%20OpenRoaming%20client%20on%20your%20proxy
[15] https://wiki.geant.org/pages/viewpage.action?pageId=133763844