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

(work in progress)

Service Provider settings

Also see Passpoint / Hotspot 2.0

OpenRoaming ANPs

Participating in OpenRoaming as an ANP means

a) having a compatible Wi-Fi infrastructure that supports OpenRoaming

b) adding a number of Passpoint Roaming Consortium Organization Identifiers (RCOIs) in the beacons of the Wi-Fi network and

c) to have an uplink into the OpenRoaming RADIUS infrastructure.

Wi-Fi Infrastructure

To be able to use OpenRoaming, you must use access points (APs) that support Hotspot 2.0 (Passpoint), which OpenRoaming relies on. This means your APs must support ANQP, standardised as 802.11u. Some vendors will not mention whether Hotspot 2.0 is supported in their AP. APs geared towards home networks (so, consumer-level) tend to not have it. If in doubt, contact the vendor.

Enterprise-level APs tend to have support for ANQP and also for Hotspot 2.0. Again, if in doubt, please contact the vendor first and verify that the AP will support it before you purchase. The Release version of Passpoint is described here: https://source.android.com/docs/core/connect/wifi-passpoint

Vendors that do support Hotspot 2.0 are Aruba, Meraki, Cisco (obviously) and Ubiquiti. This list is not exclusive. We know that some vendors are categorically not supporting Hotspot 2.0.

Some vendors only make Hotspot 2.0 features available on request. One example is Meraki, where you must contact support through the Meraki online management portal to request that Hotspot 2.0 is enabled.

RADIUS Server

Your own RADIUS server can be anything, but if you have a RADIUS server that can speak Radsec, you'll be well on your way there. Radsecproxy is arguably the most well-known open-source Radsec server (and you can put it in front of other non-Radsec servers like Microsoft's NPS) and it is actively supported by the eduroam community; FreeRADIUS 3.2.x has vastly improved Radsec support over earlier versions (you're strongly encouraged to move to the v3.2 branch). Radiator, Cisco ISE and Aruba ClearPass are paid-for solutions that support Radsec, with Radiator very well-suited to do dynamic routing. If you know of other software that supports Radsec, let us know!

If you are a WBA member, populate the Operator-Name RADIUS attribute with your WBA ID in this format: `4<WBA ID>`, e.g. `4EDUROAM`, or `4JISC:GB`

If you are not a WBA member, you will not have a WBA Identifier, so you should probably use `4EDUROAM` to indicate you are an eduroam member. Alternatively, if your NRO is a WBA member (the UK NRO Jisc is), they will likely assign a WBA sub-id to you.

You are required to pop a Chargeable-User-Identity request into your Access-Requests. If you are unable to do this, your uplink can potentially do this. The UK OpenRoaming proxy does this by default.

Beacon Settings

In order to signal that eduroam users are welcome, a set of these RCOIs can be used. Below are two common choices. Note that the SSID for the network is then arbitrary but SHOULD NOT be "eduroam" as there are known side-effects on supplicants when the network configuration matches both by SSID and by RCOI.

- **Baseline Participation:** OpenRoaming for All Identities, settlement-free, no personal data requested, baseline QoS - includes, but is not limited to users in education and research
  5A-03-BA-00-00 - usage of the hotspot is governed by the OpenRoaming End-User Terms and Conditions
- **Education-Only Participation:** OpenRoaming Visited Network Providers who want to signal that they specifically welcome educational and research (i.e. eduroam) visitors settlement-free, should add the following RCOI instead:
  5A-03-BA-08-00 - usage of the hotspot is governed by the OpenRoaming End-User Terms and Conditions
  (this option makes sense if the hotspot is also welcoming other identities but on different terms, e.g. with-settlement)
- The OpenRoaming framework allows announcing better QoS levels ("Silver" and "Gold") which come with their own RCOIs, differing from the above in one hexit. Since there is no benefit for an ANP in giving higher guarantees, it is suggested not to announce those RCOIs.
- **Note, as of 8 Feb 2021**: some onboarding tools and IdPs still use exclusively the pre-standard RCOI from Cisco times. This includes most notably: Cisco "OpenRoaming" app; the Samsung OneUI onboarding workflow. If you want to support users with IdPs served by these tools, be sure to include the RCOI **00-40-96** in the beacon.
- You can calculate other RCOIs supported by OpenRoaming here: https://wireless-broadband-alliance.github.io/OR-rcoi-config/

Uplink

In order to be able to communicate with OpenRoaming, you have to either set yourself up as an OpenRoaming service provider (called an ANP in OpenRoaming land) by applying for a certificate from the Wireless Broadband Alliance (WBA), or you have to connect your server to an uplink (a proxy that gets you access to the OpenRoaming network).

- Third-party hotspots which are onboarded in the OpenRoaming ecosystem by a third party need to take no further action. An OpenRoaming ANP uses the normal NAPTR discovery for users from an eduroam realm. This means that eduroam IdPs will need to publish a NAPTR record (see further down) and have it point to an eduroam OpenRoaming ANP proxy. (eduroam OT provides one such proxy for all eduroam participants; eduroam NROs may provide their own for their own institutional user base).
- Existing eduroam hotspots wishing to make use of eduroam infrastructure as their OpenRoaming uplink provider currently need to connect the Wi-Fi network that has these RCOIs to a proxy run by the eduroam Ops Team - contact points for this are Paul Dekkers and Stefan Winter. Alternatively, contact the UK NRO Jisc, who also operate an eduroam OpenRoaming ANP proxy.
- If you intend to be an ANP, depending on your network access provision conditions, you may need to arrange for additional network provision that allows you to route network traffic that does not comply with your existing provision conditions. For example, organisations receiving network access through the UK JANET network must ensure that non-research/educational users are not routed over the existing network connection, but via separate network access (such as a broadband connection from a commercial provider).
- Also, if you intend to be an ANP, you must forward accounting requests to your uplink, and they are required to send those on to the identity provider.

Optional mobile network wireless offload

Mobile networks can use OpenRoaming to off-load wireless activity. Currently, only a very limited number of mobile carriers on the planet support this option. This ability is configured using the MCC/MNC Passpoint 2.0 options. The values for the MCC and MNC values can usually be derived from the '@wlan.mncXXX.mccYYY.3gppnetwork.org' username you can see on a network, any 0 prefix can be dropped. AT&T for example has two pairs, '310 280' and '310 410', while T-Mobile USA has one: '310 260'. The planet's MCC and MNC values can be looked up at https://mcc-mnc.net/

To date we are aware that in the US, AT&T and T-Mobile configure their SIMs to use OpenRoaming if their MCC/MNC pair is advertised, but we're also aware that Swisscom also potentially supports this. If you have a Swisscom phone, please let us know whether you can make this work!

Access Point Configuration examples

The configuration snippets that enable OpenRoaming with the "OpenRoaming All" and an uplink to the eduroam OT proxy are on the following pages:

ArubaOS 8.x (stand-alone)

ArubaOS 8.x (controller-based)

Cisco IOS-XE

FortiWiFi or FortiAP

Meraki OpenRoaming (cloud controller managed)

Ubiquiti UniFi OpenRoaming (Network controller managed)

eduroam SPs

Beacon Settings

Hotspots which want to become eduroam SPs but cannot use the SSID "eduroam" should use the eduroam Roaming Consortium Organisation Identifier (RCOI)

00-1B-C5-04-60 [configured in end-user device to be displayed as: "eduroam®"]

to indicate that their Passpoint network is willing to accept eduroam guests.

Uplink

For the actual request routing, there are three possible ways:

1. negotiate a RADIUS AAA server address and shared secret with an eduroam NRO, to be used as uplink for authentications. Then, either
   1a) send all realms not belonging to another roaming partner to the eduroam servers (a "default" routing to eduroam). This is only possible if all other roaming partners at the hotspot are identifiable and can be enumerated.
   1b) use equipment that supports Passpoint R3 to allow identifying and forwarding of the thousands of realms in eduroam towards that one server (by leveraging the then-present RADIUS attribute "HS2.0 roaming consortium" [Vendor-Specific, Vendor 40808, Attribute 6] in the authentication request).
2. get a roaming certificate for usage with RADIUS/TLS and Dynamic Server Discovery (e.g. from eduroam Operations directly) and look up DNS NAPTR records for the realm in question; the NAPTR labels being "x-eduroam:radius.tls" (if you have a RADIUS/TLS server certificate from eduroam) or "aaa+auth:radius.tls" (if you have any other server certificate). Connections should be attempted to all servers resulting from the respective DNS responses. Note: only a minority of eduroam IdPs currently use NAPTR records; not all eduroam realms will be reached with this configuration.

1a) is currently the most viable option.

Note for existing eduroam SPs based on SSID

There are currently no plans to move away from using the **SSID** "eduroam" as the single user-facing identifier for hotspots operated directly by an eduroam participating organisation. ~~If this ever changes, the Roaming Consortium Organisation Identifier~~

~~**00-1B-C5-04-6F** [configured in end-user device to be displayed as: "eduroam®"]~~

~~is reserved for that purpose. It is configured in some supplicants but not expected to be emitted by any SP which has an SSID "eduroam" at this point.~~

~~However, eduroam SPs which deploy a separate onboarding SSID can benefit from the Online Sign-Up capabilities in Passpoint R2 and above. They should configure their eduroam SSID to emit the OSU (Online Sign-Up) portions of Passpoint and configure the OSU server URL as defined below as the target server for Online Sign-Up. Their onboarding SSID must then allow access for end-users to that URL and to eduroam CAT.~~

Identity Provider settings

eduroam Identity Providers interested in letting their users authenticate in a third-party roaming scenario may need to implement some elements of the eduroam Service Definition which are typically only optional.

OpenRoaming

In particular, for participation in OpenRoaming, the following is REQUIRED:

- The contact information concerning the Identity Provider in the eduroam Operations Database MUST be complete and accurate, including at least email address, postal address and telephone number
- The Identity Provider MUST generate Chargeable-User-Identity attributes in authentication responses
- The DNS zone for the Identity Provider's realm name MUST include a NAPTR record for their realm pointing to an eduroam OpenRoaming interchange proxy. The example below targets the general-purpose proxy operated by eduroam OT; the target host may be different for eduroam NROs who operate their own proxy:

  ```
  realm.name. 43200 IN NAPTR 100 10 "s" "aaa+auth:radius.tls.tcp" "" _radsec._tcp.openroaming.eduroam.org.
  ```
- End user devices need to be provisioned with the pertinent settings to recognise OpenRoaming hotspots - see section "End-User Device Settings" below
- The end users themselves need to be made aware that they are bound by the OpenRoaming End-User Terms and Conditions whenever they connect to OpenRoaming hotspots.

When your user is actually roaming with OpenRoaming, this is visible in the RADIUS datagrams due to the RADIUS Attribute

```
Operator-Name = 4<string>
```

where the `string` is the WBA Identifier of the organisation that operates the hotspot.

End-User Device Settings

Starting with version 2.1, the eduroam onboarding toolset (eduroam CAT and eduroam Managed IdP) integrates Passpoint network definitions in general, and OpenRoaming settings in particular, in its standard workflow. This version is currently available *for testing* on https://cat-test.eduroam.org with a stale copy of production data.

CAT eduroam Passpoint settings

CAT automatically injects network definitions based on the eduroam Roaming Consortium Organisation identifier (RCOI **00-1B-C5-04-60** with the Display Name "eduroam®") on all platforms where this is possible and does not create nuisances for end users.

CAT OpenRoaming settings

When their eduroam NRO has enabled the feature set in their country's tenancy (which they do by setting "OpenRoaming: Allow Organisation Opt-In" in their NRO settings), eduroam IdPs can easily have CAT create OpenRoaming enabled installers by adding a single attribute in the "Media-Specific" category. This will include the RCOIs **5A-03-BA-00-00** "OpenRoaming for All Identities, settlement-free, no personal data requested, baseline QoS") and **5A-03-BA-08-00** ("OpenRoaming for Educational or Research Identities, settlement-free, no personal data requested, baseline QoS") in the installers. The attribute is called "OpenRoaming" and can take one of four values:

Value	Meaning
Ask User	During download on the web interface, users will be actively asked whether they want to have OpenRoaming access included in their installer (on platforms where OpenRoaming installation is technically feasible). They are shown and need to acknowledge the OpenRoaming T&Cs before the download starts. Where not technically feasible, users will get a standard eduroam installer download and won't see the OpenRoaming T&Cs.
Ask User, T&Cs pre-agreed	During download on the web interface, users will be actively asked whether they want to have OpenRoaming access included in their installer (on platforms where OpenRoaming installation is technically feasible). By selecting this value, the IdP asserts that their end users have already seen and accepted the OpenRoaming T&Cs; the download flow does not repeat this acknowledgement. Where not technically feasible, users will get a standard eduroam installer download and won't see the OpenRoaming T&Cs.
Always	Include the OpenRoaming access details in all installers (where technically feasible). The users are shown and need to acknowledge the OpenRoaming T&Cs before the download starts. Where not technically feasible, users will get a standard eduroam installer download and won't see the OpenRoaming T&Cs.
Always, T&Cs pre-agreed	Include the OpenRoaming access details in all installers (where technically feasible). By selecting this value, the IdP asserts that their end users have already seen and accepted the OpenRoaming T&Cs; the download flow does not repeat this acknowledgement. Where not technically feasible, users will get a standard eduroam installer download and won't see the OpenRoaming T&Cs.

Device support

Windows before 10

These platforms are not configured for Passpoint.

Windows 10 and Windows 11

Both for eduroam CAT and eduroam Managed IdP, the eduroam Passpoint profile is always included and the OpenRoaming Passpoint profile is optionally included. Installation of these may fail if the chipset and driver on the machine does not support Passpoint. Such failures are silently ignored (and only the eduroam SSID configuration is then installed); no user inconvenience.

Apple (Mac OS X, macOS, iOS, iPadOS)

For eduroam Managed IdP, eduroam Passpoint-based profiles are always installed alongside the SSID-based ones. This is expected to work throughout the product palette of Apple, and with no additional user interaction. OpenRoaming is not currently enabled on Managed IdP.

eduroam CAT Mobileconfig files will install OpenRoaming Passpoint profiles when enabled (all EAP types); it will however only install the eduroam Passpoint profile if the IdP's chosen EAP type is "EAP-TLS". This is because of known user nuisances regarding multiple username/password prompts for multiple SSID and Passpoint profiles which CAT minimises by omitting that extra prompt for eduroam Passpoint.

Geteduroam will install an OpenRoaming profile if the configuration exists.

Android

eduroam Passpoint profiles and the optional OpenRoaming Passpoint profiles can be installed only with the new geteduroam app (i.e. not with the predecessor "eduroamCAT"). geteduroam has varying support for Passpoint profiles depending on the Android version and whether the IdP chose "Ask" vs. "Always" - the "Always" variant currently has better support across all supported Android versions; "Ask" support needs special IdP workarounds.

Intrinsic support for OpenRoaming exists on later (read, newer) devices and versions of Android. For example, recent Google Pixel devices (Pixel 5 and later) show "OpenRoaming" as a network when a HS2.0 hotspot is detected. You then have the choice to enable roaming to this network by choosing to use your Google account associated with your Android phone. Apps like 'Cisco Openroaming' also enable an account on the same network. CAT profiles installed with geteduroam will show "<realm name> via Passpoint" instead but do not associate with the "OpenRoaming" SSID. On some Samsung devices, you may see "OpenRoaming available using Samsung Account" instead, which will function in a similar fashion as the Google Pixel.

Geteduroam will install an OpenRoaming profile if the configuration exists. It will show as 'your realm via Passpoint' in your Wi-FI network list.

Linux

Any recent version of wpa_supplicant supports Passpoint, provided it has been built with the `CONFIG_INTERWORKING=y` and `CONFIG_HS20=y` flags. Check your Linux distribution's build source configurations for confirmation. Instead of using a `network {}` block (as you would with a standard 802.1x network), you use the `credential {}` block.

To enable Passpoint roaming, set `interworking=1` and `hs20=1` in your wpa_supplicant.conf, and provide the credential block to use.

More information is available at https://github.com/xradvanyip/hostapd-openwrt/blob/master/wpa_supplicant/README-HS20

ChromeOS

Recent versions of ChromeOS should also support Passpoint. Google is active in the Passpoint community. You should be able to use the geteduroam app for Android on ChromeOS to configure your ChromeOS device for Passpoint.

Infrastructure

OpenRoaming

eduroam currently operates a beta-quality central interchange point with OpenRoaming. Third-party SPs find it automatically by looking up NAPTR records in DNS for aaa+auth for the respective realm. Identity Providers need to configure a NAPTR record, see above.

UK eduroam operator Jisc also operates a beta-quality central interchange point with OpenRoaming. eduroam(UK) members should contact their eduroam helpdesk to gain access and join the trial.

Passpoint Release 2: Online Sign-Up

eduroam plans to operate an OSU server which directs unprovisioned end-users to the eduroam CAT toolset. The provisional URL for this server is

```
https://cat-osu.eduroam.org/soap/?idp=X
```

Where to see OpenRoaming in action

OpenRoaming locations, given relative 'novelty' of the technology and its growth, are still somewhat sporadic, depending on location.

The Wireless Broadband Alliance took the eduroam Map as an example (encouraged by eduroam community members) to publish its own map at https://wballiance.com/openroamingmaps/

This map uses the WiGLE service to use crowdsourced data to populate the map and is generally accurate within 24 hours. Non-residential locations generally show up as clusters of at least 4 pins together (a pin per band per SSID).

Policy

GeGC to decide on terms and conditions for letting random SPs serve eduroam users.

Back to top