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

(work in progress)

Service Provider settings

OpenRoaming ANPs

Participating in OpenRoaming as an ANP means

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

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

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.

Uplink

- 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. eduroam IdPs will need to publish that NAPTR record 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 eduroam OT - contact points for this are Paul Dekkers and Stefan Winter

Access Point Configuration examples

ArubaOS 8.x

The configuration snippets that enable OpenRoaming with the "OpenRoaming All" and an uplink to the eduroam OT proxy are on this separate page.

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® Hitchhiker" (name provisional)]

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 needs to 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 is 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 2.0.3, the eduroam onboarding toolset (eduroam CAT and eduroam Managed IdP) automatically inject network definitions based on the eduroam Roaming Consortium Organisation identifiers (RCOI) on all platforms where this is possible. The platforms and their respective caveats are listed below.

In general, the Passpoint configuration configures two eduroam RCOIs:

00-1B-C5-04-60 [Display Name "eduroam® Hitchhiker" (name provisional)]
00-1B-C5-04-6F [Display Name "eduroam®"]

The latter one is reserved for a distance-future use, in case eduroam would go fully Passpoint and give up on SSID-based configurations throughout all SPs world-wide. The RCOI would then signify eduroam self-operated hotspots with this "home" display name.

To allow your users to connect also to OpenRoaming hotspots (under the OpenRoaming End-User Terms and Conditions), firstly make sure that your users acknowledge the OpenRoaming End-User Terms and Conditions. Then configure the following six RCOIs additionally:

5A-03-BA-00-00, 5A-03-BA-10-00, 5A-03-BA-20-00 (a.k.a. "OpenRoaming for All Identities, settlement-free, no personal data requested, baseline/silver/gold QoS) - usage of the hotspot is governed by the OpenRoaming End-User Terms and Conditions

5A-03-BA-08-00, 5A-03-BA-18-00, 5A-03-BA-28-00 (a.k.a. "OpenRoaming for Educational or Research Identities, settlement-free, no personal data requested, baseline/silver/gold QoS) - usage of the hotspot is governed by the OpenRoaming End-User Terms and Conditions

Windows before 10

These platforms are not configured for Passpoint.

Windows 10

Both for eduroam CAT and eduroam Managed IdP, the SSID-based and the Passpoint profile are installed in sequence. The SSID based configuration always succeeds. Installation of the Passpoint profile may fail if the chipset and driver on the machine does not support Passpoint. Such failures are silently ignored; no user inconvenience.

As of October 2019, there are field reports that some 10-20% of devices which do claim Passpoint support and which will be configured with Passpoint do not actually work post-config. These failures are occuring for all Passpoint configurations, i.e. are independent of eduroam; but they also do not cause any harm to the end user - the authentication and connection to Passpoint networks is simply not possible then. Up-to-date drivers are reported to help in such situations.

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

For eduroam Managed IdP, 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.

For eduroam CAT, Passpoint configuration is only installed if the IdP's chosen EAP type is "EAP-TLS" as this EAP type does not trigger multiple prompts for usernames and passwords. For all password-based EAP methods, only the SSID-based configuration is pushed to the device. Apple personnel is aware of the annoyance of multiple username/password prompts and installation of Passpoint configurations alongside SSID-based ones will be enabled as soon as the situation ameliorates.

Android

The eduroam CAT app needs an update to support configuring Passpoint networks.

(The built-in method of Passpoint R1 provisioning as described in AOSP: Wi-Fi Passpoint R1) is not generally usable as the installation of new, dedicated Wi-Fi root CAs is prohibited by Android API.)

Linux

TBD.

ChromeOS

TBD.

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.

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
```

Policy

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

Back to top