

== NPS 2008R2 eduroam config to prevent Access-Requests with malformed username from being forward to the JANET NRPS ==

Phil Mayers, Imperial College London

Home sites: you should create client entries for each NRPS under the "RADIUS Clients" section; be sure to set their "Friendly Name" to NRPS1, NRPS2, NRPS3 etc. so you can match them below.

Visited sites: you should create group called "NRPS" in the "Remote RADIUS Server Groups" section. Add the 3 NRPS IPs and set their secrets.

You should then create the following connection policies, in this order:

(1, Home sites only)

1. Client-Friendly-Name matches ^NRPS.*
n.b. NO extra conditions here - accept all from NRPS
Authenticate locally

(2 & 3, Visited sites only)

2. User-Name matches ^([\^@]*)@yourrealm\.ac\.uk\$
Plus matches required to limit to eduroam (see below)
Authenticate locally
3. User-Name matches ^([\^@]*)@[-a-zA-Z0-9]+(\.[-a-zA-Z0-9]+)+\$
Plus matches required to limit to eduroam (see below)
Forward to NRPS

== Limiting matches to eduroam ==

Because NPS doesn't offer any conditional/branching features, or a way to bind a client/group to a set of policies, you have to be careful to make sure your policies match appropriately.

In the case of a Home site, you should accept everything from the NRPS - that is, only match on the "Client-Friendly-Name" that you've given to the NRPSes.

In the case of a Visited site, you may be using your NPS server for other things (e.g. VPN, non-eduroam Wi-Fi). In that case, you will need to make your Visited site policies (2 & 3, above) only apply for eduroam authentication.

A common way to do this if your wireless platform sends attributes of the form:

Called-Station-Id = 00-11-22-33-44-55:eduroam

...is to add the following matches to policies 2 & 3:

Called-Station-Id matches .+:eduroam\$

If your NPS server is dedicated to eduroam use, you can omit this match.

HOWEVER: it is important that you **NOT** add a 4th policy saying:

4. No conditions
Authenticate locally

If you do this, your users will be able to configure eduroam at home using "username" when they should be using "username@yourrealm.ac.uk", and it will fail for them when they leave.