

2022-01 Advisory: Reinstatement of Roaming2 NRPS

Released: 6th January 2022

This advisory is important and relevant to all eduroam(UK) service organisations.

- Background and scope
- Phase 1
- Phase 2
- Monitoring Progress
- Summary
- Action required
- Supplementary Information

Background and scope

The eduroam(UK) team is in the process of migrating all national roaming proxy servers (NRPS) to Jisc shared infrastructure. This migration has taken some time, not helped by the pandemic, but it is now at the point where we would like all eduroam service administrators at member organisations to prepare for the migration of roaming2.ja.net. The migration of roaming1.ja.net will follow shortly afterwards, date to be advised.

The move to the new platform involves a necessary IP address change - which also enables us to better manage our IP address space and provides for future development of the service.

We intend to start with roaming2.ja.net since the return to a three-server national RADIUS infrastructure is a high priority and due to the fact that roaming2 has been out of service for some time, the status of the server in member organisations' RADIUS servers (ORPS) configurations requires review and the change of IP address can form part of that process.

The existing shared secrets for the reinstated roaming2 **will not** change and are displayed for administrators via the RADIUS servers configuration panel on the eduroam(UK) Support Server (ESS) portal.

The necessary IP address change for roaming2.ja.net is as below:

Old IPv4 Address: 194.83.56.249

Old IPv6 Address: 2001:630:1:129::249

New IPv4 Address: 193.63.195.50

New IPv6 Address: 2001:630:1:133::50

Phased migration: To ensure minimal risk to existing service levels, this migration will be taking place in two phases in rapid succession: firewall and roaming2 client configuration go-

live by **1st February 2022** and roaming2 authenticator go-live on **1st March 2022**.

We recognise that the above timeframe is tight, especially for organisations which may have lengthy change control processes to follow, but it is hoped that it is achievable.

The new IP addresses for roaming2.ja.net are already in place and are accepting traffic but ***you should only send visitor test authentications until the go-live date***. We intend to decommission the old IP addresses (and update DNS for roaming2.ja.net to the new IP addresses) on the second date in this advisory.

Basic updating instructions: For the most commonly used RADIUS server products in the UK are included as supplemental information at the end of this advisory.

Customers of Jisc Trust & Identity Group's retained expertise consulting services: We will work with our colleagues in the Trust & Identity group to have you switched over on schedule.

Notice of Migration of roaming1.ja.net: Migration of a second NRPS to the Jisc shared infrastructure is provisionally scheduled for around the Easter break (dates to be confirmed). We intend to follow a similar protocol as described in this advisory to migrate roaming1.ja.net - after the reinstatement of roaming2.ja.net is deemed to be complete.

Roaming0.ja.net: Roaming0 remains in service, unchanged. The migration of Roaming2 and Roaming1 are the most urgent of the infrastructure upgrades. Migration of Roaming0 will take place in due course after the current moves are complete and we'll be making an announcement in the future.

Queries/comments: The **eduroam clinics on 1 February and 1 March 2022** will be dedicated to this transition process, with the eduroam(UK) team on hand to discuss any problems you may encounter, and you can also lodge a support ticket with our help desk by e-mailing help@jisc.ac.uk ^[1] with your query, or by using the support form at <https://www.jisc.ac.uk/forms/eduroam-support-request> ^[2].

Phase 1

The work described below may be commenced now. The deadline for completion of this phase is 1st February 2022.

If your firewall, ORPS and/or NAT configurations are hostname-based, you may use the hostname **hv1-roaming-002.eduroam.virt.ja.net** as interim until the Phase 2 deadline below on which date you must change the hostname to roaming2.ja.net. We will adjust the DNS TTL for the Phase 2 deadline to be short to assist in a fast transition to the new IP address.

Applicable to ALL member organisations, IdPs and SPs (Home, Home-and-Visited and Visited only):

a) Configuration of your firewall to accept/send traffic (UDP/1812) and accept ICMP from the new IP addresses and you must ensure that any NAT rules are updated to forward traffic from the new IP addresses to your ORPSs and vice versa.

Applicable to IdPs (Home and Home-and-Visited) member organisations:

b) Configuration of your RADIUS servers to include the new IP addresses for roaming2.ja.net as a **client** in your ORPSs; add and enable the new addresses to your clients config so that any RADIUS traffic sent from the new IP addresses will not be ignored by your RADIUS servers. (Check your Configure page on Support Server for the shared secrets - which are not changing).

The above steps are necessary to ensure that any traffic sent by the new roaming2.ja.net will reach your ORPSs and not be lost. If authentication requests arising from your roaming users are sent via roaming2.ja.net but do not reach your ORPS, the request will not complete, the user authentication will fail and the following message will appear in your ESS portal RADIUS error log:

roaming2 : No working hosts in AuthBy for Identifier <your realm>, sending reject to clear backlog

Testing - you can use the roaming user authentication test on your Troubleshoot page on Support server to check that RADIUS requests can get through to your ORPS once you have made the above changes (select 'roaming2' from the dropdown list on the blue Tests panel top line).

Phase 2

Between 1st - 28th Feb you should prepare your configuration ready for implementation on the go-live date of 1st March.

Applicable to all SPs (Home-and-Visited and Visited only) member organisations:

Configuration of your RADIUS servers to add and enable the new IP addresses above as a remote RADIUS server (proxy/authenticator) in the configuration of your ORPS, so that your RADIUS servers can use the new Roaming2 server to send authentication requests to from your eduroam visitors.

You may wish to implement both Phase 1 and 2 at the same time, but until such time that everyone has changed the configuration of their RADIUS servers, higher error rates will occur for authentication requests handled by roaming2.ja.net as these may be sent to ORPSs not as yet configured to accept requests from roaming2.ja.net. Therefore we advise that you do not enable the server portion of your configuration before the Phase 2 go-live date.

The deadline go-live date for this phase is **1st March 2022**. The DNS IP address records for roaming2.ja.net will change on this day.

Monitoring Progress

It is essential that all member organisations implement the required changes since all member ORPS form part of the RADIUS server hierarchy with the eduroam(UK) national proxy servers as key components. The performance of the service is reliant on the integrity of the RADIUS hierarchy.

In February, between Phases 1 and 2, using the roaming user test system on ESS, the

eduroam(UK) team will actively monitor connectivity from the new roaming2.ja.net IP address to ensure that no organisation is left behind, and we will actively follow up by e-mail and, closer to the Phase 2 date, by phone.

After the Phase 2 deadline, we will actively monitor traffic on the new server to see whether any organisations are not sending any traffic, and actively follow up with these organisations to check that this work has been completed.

Summary

- Update your firewall, NAT rules, and RADIUS servers to allow incoming RADIUS (UDP) traffic from the new IP addresses for roaming2.ja.net as above by **1st February 2022**.
- Update your RADIUS servers to enable sending traffic to the new IP addresses for roaming2.ja.net as above by **1st March 2022**. The old IP addresses will cease on this date.

Action required

Two dates apply to this advisory: **1st February 2022** and **1st March 2022**.

By the first date, you **should have** registered the new **IP address 193.63.195.50 (and its IPv6 counterpart 2001:630:1:133::50)** as a client on your ORPS(s) and you must have configured your firewall(s) and any NAT rules for incoming traffic from these IP addresses. You may opt to delay this action until the **second date**, but the eduroam(UK) team will be actively contacting organisations who have **not** completed this action before the second date.

By the second date, you **must have** registered the new IP addresses above as a remote RADIUS server (proxy/authenticator) on your ORPS(s), as on the second date the existing IP addresses for roaming2.ja.net will be decommissioned. The eduroam(UK) team **will** contact your organisation if no traffic relevant to your organisation has been seen on the new IP address.

Supplementary Information

Microsoft NPS

Before **1st February 2022**, open your NPS console, select 'RADIUS Clients and Servers', then select 'RADIUS Clients'. Within the list of clients, look for a client with the IP address '194.83.56.249'. This is the old roaming2.ja.net IP address. If you followed the Jisc NPS Guide, you may have called it 'roaming2' or 'roaming2.ja.net'. Double-click this host, click the 'Address' field and amend it to the new IP address of '**193.63.195.50**'. If you also defined this server as a Template (to use it as both a client and a server), you may need to amend the template instead. For this, go to Templates Management, then look in the RADIUS Clients and Remote RADIUS Servers template groups for the server to amend it.

If you did not add roaming2 originally, please do so by following the Jisc NPS Guide from Page 41 (Section 11) onwards with the new IP address and your existing secret for the server. See

[https://support.eduroam.uk/files/eduroam\(UK\)%20Microsoft%20NPS%20Configuration%20Guide.pdf](https://support.eduroam.uk/files/eduroam(UK)%20Microsoft%20NPS%20Configuration%20Guide.pdf)
[3]

Restart NPS by right clicking the top entry (with the globe), choosing 'Stop Service', and then, after 15-30 seconds, repeating the action and choosing 'Start Service'.

On or before **1st March 2022**, you must also adjust your 'Remote RADIUS Server' group (under the 'RADIUS Clients and Servers' option, in 'Remote RADIUS Server Groups'). See section 14 in the NPS guide. Add the server (in a similar fashion as above in the 'RADIUS Servers' option). Click on the Load Balancing tab and check the timeouts and weighting. You may wish to change the priorities around as currently roaming0.ja.net is the most used as it is first in line for most organisations and you may wish to take advantage of a lower service load on the new server.

FreeRADIUS

Before **1st February 2022**, we suggest you amend your existing '**client**' stanza for roaming2.ja.net in the **clients.conf** file (on RedHat/CentOS in /etc/raddb/, on Debian in /etc/freeradius, on Ubuntu in /etc/freeradius/3.0/) to use the new IP address '**193.63.195.50**'. If you do not have an existing entry, copy the entry for roaming1.ja.net and adjust it with the new IP address and the correct secret from the ESS portal. You may also wish to add the IPv6 address if you prefer it.

On or before **1st March 2022**, to add roaming2.ja.net as a server, modify the **proxy.conf** file in the same location as clients.conf above, and adjust the existing '**home_server**' stanza for roaming2.ja.net there, if you have one. If you do not have one, duplicate the one for roaming1.ja.net and amend it accordingly with the new IP address and the secret from the ESS portal. Then also add an entry for the new server into the '**server_pool**' stanza that includes roaming0.ja.net and roaming1.ja.net.

Then restart your instance of FreeRADIUS for changes to take effect.

Cisco ISE

Before **1st February 2022**, configure the new roaming2.ja.net as a Network Device in ISE. Go to Network Resources, Network Devices to define a new network device with the new IP address for roaming2.ja.net, '**193.63.195.50**'. For ease of use in the future, simply call it roaming2.ja.net or something similar. Give it the secret for roaming2.ja.net as described in the ESS portal.

On or before **1st March 2022**, you should configure roaming2.ja.net as an external RADIUS server. Go to Administration, Network Resources, External RADIUS Servers, and then either Add (if you never added roaming2) or Amend your entry (if you added it originally with the old IP address) for roaming2 with IP address '**193.63.195.50**'. Also go to RADIUS Server Sequences and adjust the priorities accordingly to take advantage of the fact that roaming2 should have less load on it.

Aruba ClearPass

Before **1st February 2022**, you should configure roaming2.ja.net as a new Network Device. Go to Configuration, Network, Devices. If you already have an entry in the table for roaming2.ja.net, click it and amend the IP address to '**193.63.195.50**'. If you do not have an entry, please add one by clicking on the + in the top right corner and follow the prompts to set it up with the new IP address. Do not enable RadSec or RADIUS CoA.

On or before **1st March 2022**, you should configure roaming2.ja.net as an external authentication source. Go to Configuration, Authentication, Auth Servers. In the table you may already have an entry for roaming2.ja.net. Please adjust this with an updated IP address of '**193.63.195.50**'. If you do not have an entry, please add one by clicking on the + and filling in the new details. You should follow the recommended guidance as per the Aruba manual to adjust timeouts.

Source URL: <https://community.jisc.ac.uk/library/network-and-technology-service-docs/2022-01-advisory-reinstatement-roaming2-nrps>

Links

[1] <mailto:help@jisc.ac.uk>

[2] <https://www.jisc.ac.uk/forms/eduroam-support-request>

[3] [https://support.eduroam.uk/files/eduroam\(UK\)%20Microsoft%20NPS%20Configuration%20Guide.pdf](https://support.eduroam.uk/files/eduroam(UK)%20Microsoft%20NPS%20Configuration%20Guide.pdf)