FAQs for eduroam System Administrators and Implementation Techs - Part 1

This page lists the most common frequently asked questions about eduroam in the UK. The table of contents summarises the questions asked; please scroll down to the relevant section for the answer. See Part 2 if your question is not addressed here.

Last updated: 24/07/19

Contents:

1) 802.1X and EAP
   - What is 802.1X and EAP and how do they work?
   - Give me one example of how EAP-TLS is preferrable to PEAP/MSPCHAPv2 or EAP-TTLS/PAP

2) Networking issues / Application & Interception Proxies / Firewall configuration / Ports and protocols
   - Is web content filtering permitted on eduroam services?
   - Can TLS/SSL interception proxies (for instance as used in content filtering) be deployed?
   - Can users' traffic be monitored and analysed?
   - Is PPTP considered secure and can it work with NAT?
   - We can authenticate and get connected to eduroam ok, but client states "no internet" and we can't access web pages?

3) Joining eduroam / Realms / Eligibility
   - Can individuals join eduroam?
   - Can a person have an eduroam ID without host org joining eduroam?
   - Is eduroam available to all members of an organisation?
   - Can alumni have eduroam accounts?
   - Do users need to have a network logon account? What about access for the public/non-registered users?
   - Can we have an additional top level realm for our organisation?
   - Can sub-realms be configured for an organisation?

4) RADIUS server software and configuration
   - Links to the various RADIUS server software websites
   - How many RADIUS client devices can my ORPS support?
   - What RADIUS server software are other eduroam participants using?
   - Known issues with particular versions of RADIUS server software
Do you have any example configurations for Radiator?
Do you have any example configurations for FreeRADIUS?
What is unlang?
Where can get up to date binaries for FR2.2 for Centos, which ships with an old version?
Microsoft IAS implementation advice
Our AD usernames don’t match eduroam username format, how can I strip/modify realm for authentication?
Cisco ACS implementation advice
What Attributes should I NOT filter out?
What procedure do I need to follow for changing the IP address of our ORPS?
IP Addresses/FQDNs/shared secrets for ORPS - replacing ORPS and moving to a new location
Shared secrets for ORPS - internal RADIUS servers
Does Microsoft NPS support RADIUS accounting and how to avoid forwarding accounting packets to NRPS?

5) Server Certificates for ORPS

- Can I use a self-signed certificate for our RADIUS server?
- Use of Jisc Certificate Service
- Can I use the same certificate for more than one ORPS?
- How to configure client workstations to use the JCS TERENA/QuoVadis certificates
- Technical documentation on using MS IAS and Jisc SCS
- Our server certificate is about to expire! What do we do?

6) Integration of RADIUS server with back end user database

- EAP-PEAP authentication against Novell Directory Services
- FreeRADIUS integration with Active Directory
- Radiator integration with Active Directory
- Realm name not in AD - can we get NPS to translate realm?

7) Authentication Issues

- Is machine authentication permitted a) for roaming users b) for devices that will only connect on campus/at corporate office?
- How can we differentiate between institution-owned/managed devices and user-owned devices, for the purpose of managing the network environment the device is connected to after user authentication?
- When network passwords are changed the cached credentials on user devices have to be manually updated which sometimes creates issues for users
- Can't get Visited service to work - NRPS do not appear to be responding/ignoring our ORPS/blocking auth requests

8) eduroam Policy Related Issues and Dealing with Virus/Copyright Breach Incidents

- Clarification of Jisc eduroam(UK) Policy and Tech Spec on visitor logging
- Notification of Home organisations in case of visitor abuse of Policy
- Dealing with a virus incident involving an eduroam visitor

9) RADIUS Server log Keeping, Interpreting Errors in the ORPS logs and Performance
Difficulties

- Generation of Monthly Stats on eduroam usage for Microsoft IAS/NPS
- Microsoft NPS Error 'RADIUS Client Authentication Attribute not Valid' (ID 18)
- Microsoft NPS Error 'Wrong Domain' (ID 4402)
- Peaks of re-authentications at certain times of the day/heavy auth load leading to failures and poor performance

1) 802.1X and EAP

What is 802.1x and EAP and how do they work?

- IEEE 802.1X [1] - Janet technical sheet on 802.1x outlining its benefits and describing how it works and listing currently available supplicants together with their main features and applicability.
- Extensible Authentication Protocol (EAP) [2] - Janet technical sheet on EAP, describing how it works, EAP types and implementation considerations.
- Resources about EAP and its support in the current versions of Microsoft Windows [3]

Give me one example of how EAP-TLS is preferrable to PEAP/MSCHAPv2 or EAP-TTLS/PAP

EAP-TLS, which uses certificates, has the advantage that there is not a direct correlation between the certificate and the LDAP/AD password store. Should the user’s password be changed in the LDAP/AD, the certificate on their device remains working. If you need to ban a user you would do so by blocking the certificate (eg by using OSCP) rather than by disabling their account. By doing this the user could still read e-mails sent over 3G/4G which could be used to advise them of the password change/network access lock/other reasoin why eduroam connection is not working for them. Using MSCHAPv2 notification may also help.

Users do not enter their password credential when logging on with eduroam using EAP-TLS and their password isn’t stored in cache on the device, which is a security plus, but of course with EAP-TLS you do need to have and operate a certificate management system.

2) Application & Interception Proxies / Firewall Configuration - Ports and Protocols for eduroam(UK) visitor networks

Is web content filtering permitted on eduroam services?

Filtering of web traffic both URL or content-based, whilst not encouraged, is permitted on eduroam services ? provided that TLS/SSL interception is not employed in respect of services for visitors.

Furthermore, an organisation can setup a local VLAN/network segment for its own eduroam users on which the organisation can implement any policy it choses (including web content filtering) and when users are at their home organisation, local users once authenticated, can be connected to this local VLAN (using dynamic VLAN assignment). Visiting eduroam users however must be connected to eduroam-compliant network services (refer to Technical Specification).
Can TLS/SSL interception proxies (for instance as used in content filtering) be deployed?

The Technical Specification v 1.3, whilst advising against such deployment, stated that Visited organisations may in fact install application or 'interception' proxies, provided that the fact that such a system is being used is published on the eduroam service information page. Furthermore, if a proxy is not transparent, instructions for the configuration of applications to use the proxy must be published. Version 1.3 of the specification went on simply to note that "interception proxies, often used by intrusion and virus detection systems, may result in the user experiencing unexpected network behaviour."

This policy was formed with the use of proxies such as Squid in mind. Over the past year or so the deployment of TLS/SSL interception proxies has become more popular. Such proxies are employed in some content filtering systems, particularly those filtering HTTPS content (and may also be used in some intrusion and virus detection systems). TLS/SSL interception requires the user to install a CA certificate from the intercepting organisation. This is undesirable for a number of reasons. It requires significant effort by the user. It also results in the proxy breaking the secure path between user and service. It is in effect a man-in-the-middle interception and is contrary to recommended security practice. Several web browsers will flag up the security deficiency to users, who may then discontinue their (legitimate) use of the network. The v1.3 specification advised simply that unexpected network behaviour might be experienced, and noted that significant effort would be required by the user to install certificates from (untrusted) third parties.

There is an interesting article on the pros and cons of HTTPS interception at: https://www.helpnetsecurity.com/2017/03/08/https-interception-dilemma/

The policy of eduroam(UK) has now evolved in response to the development of TLS/SSL proxies and a new version of the Technical Specification has been released. **Version 1.4 of the Tech Spec requires that TLS/SSL interception proxies are NOT permitted on eduroam network services that visiting eduroam users are connected to.**

It should be noted that organisations are not obliged to connect their own users when they are at their Home organisation to the eduroam Visitor network. Rather, local users may be connected to non-eduroam network services suited to local users as required for instance where deemed necessary for a college to implement its policies on Prevent and Safeguarding. So you would been to implement dynamic VLAN assignment such that your own users are connected to the filtered and monitored network that they currently use and visitors are connected to a non proxied/intercepted network service (aka an eduroam VLAN). This eduroam network service needs to comply with the eduroam(UK) Technical Specification.

It should also be noted that content filtering not involving interception proxies IS permitted on eduroam network services for Visitors (providing its use is advertised), although this is not encouraged.

Can users’ traffic be monitored and analysed?

Q. We are contemplating data mining of the websites visited by eduroam users (for the purpose of providing analytics on the most visited web pages and repeat visits since such metrics are very useful to our collections staff and such data would prove to be force
multipliers for much needed funding bids to demonstrate delivery of resources).

The eduroam T&Cs do not prelude the monitoring and analysis of traffic but clarification is sought on whether we can:

Log our eduroam users? outbound traffic and analyse the traffic for frequently used websites and repeat visits, given that we anonymise the data so that is not personally identifiable and delete the information when no longer needed.

A. eduroam policy does not say anything about a member organisation monitoring of use of the network. However the ability to monitor suggests that a proxy may be utilised somewhere. If so, this needs to be documented to assist Jisc in any debugging that may be required. Such a proxy must also comply with eduroam(UK)?s restrictions on the employment of TLS interception. In addition, the deployment of monitoring and analysis of traffic on the eduroam service must be advertised on the organisation's eduroam service information web page.

Moreover there are some laws that need to be complied with:

At present, the Data Protection Act 1998 requires organisations to inform users of any processing of personal data, which would include logs of IPaddr/URL etc. The organisation also needs to work out which legal basis applies to the processing (Data Protection Act 1998 section 6), and ensure it meets the relevant requirements of that basis. If the organisation is using the information for internal purposes then one option is "Necessary for the Legitimate Interests of the Data Controller" (art.6f), in which case it needs to ensure that any risk of impact on the individual is minimised *and* that any remaining risk is justified by the benefit to the organisation. There is an introduction to the different legal bases, as they will be from May 2018 under the General Data Protection Regulation, at https://community.jisc.ac.uk/blogs/regulatory-developments/article/gdpr-... [5]. That article also includes a link to the ICO's thoughts on the requirements for consent to be valid under the GDPR, which becomes relevant, because...

Things are going to get more complicated from a date that the European Commission would like to be 25th May 2018. That's their proposed start date for a new ePrivacy Regulation. The current draft of that will prohibit all uses of information relating to the use of electronic communications networks - both content and metadata - unless:

a) it's necessary for providing the network, or

b) it's necessary for securing the network, or

c) you have the individual user's positive, informed, consent.

So under the current draft, consent is likely to be their only option. The legislation is at a very early stage - the Commission have published their draft, the EU Parliament has decided which committee is going to discuss it, and the Council of Ministers has had one meeting - so there are likely to be changes. There's also the question of how that timetable relates to Brexit, which adds a further layer of uncertainty to what the UK might implement. Advice for designing a system for user monitoring, would include a contingency for a *lot* of change, or indeed having to turn it off, in a year or two's time.

Is PPTP considered secure and can it work with NAT?
Q. "eduroam network must permit TCP port 1723 and IP protocol 47 in order to support PPTP, but surely PPTP is regarded as an insecure protocol these days?"

A. Almost all protocols that people use are insecure in some way - usually due to the way that a site or system implements it. PPTP is a weaker for of VPN and, like many protocols, there are ways of attacking it - but sites/people still choose to use PPTP for basic VPN usage and that's their choice.

Q. Can PPTP be made to work with NAT?

A. PPTP and NAT can be made to work fine together - after all, PPTP works fine at most people's homes and it is commonly used to connect to work networks - most people have NAT on their home Internet services. So PPTP and NAT coexistence depends on the firewall being used and whether a site needs to activate some extra helper.... natively it won't work as the PPTP session has source/destination address - the system needs a pass-through or helper to keep track of the session.

We can authenticate and get connected to eduroam ok, but client states "no internet" and we can't access web pages.

We did an OS upgrade on our firewall and although that appears to have been successful, since then we've been experiencing this problem.

If devices can connect to eduroam then the authentication part of the system, which eduroam deals with, is running OK. The local Wi-Fi service provision on the other hand can be affected by many things. Since your firewall was upgraded recently, the chances are this is where the problem lies. Check sequence:

1) Are connected devices assigned an IP address?
If no IP address is assigned there is a DHCP issue - is the DHCP service provided by the firewall and is it running/configured correctly?

2) Are they assigned a DNS server and can they resolve URLs?
If not there's a DNS resolver issue - how are DNS resolvers made available to clients?

3) If any access to local network resources should be available, does that work?
If local access is OK then there is an internet access problem - firewall permissions for outbound traffic and any NAT config should be checked. Are the requisite ports and protocols correctly enabled?

3) Joining eduroam / Realms / Eligibility

- Can individuals join eduroam?
- Can a person have an eduroam ID without host org joining eduroam?
- Is eduroam available to all members of an organisation?
- Do users need to have a network logon account? What about access for the public/non-registered users?
- Can we have an additional top level realm for our organisation?
- Can sub-realms be configured for an organisation?
Can individuals join eduroam? / Can a person have an eduroam ID without host org joining eduroam?

No. Individuals can only use eduroam as members/associates of an organisation that itself is a member of eduroam(UK) and that acts as an identity provider, i.e. an IdP / Home service participant. The member organisation authenticates the user. eduroam(UK) does not act as an identity provider/authenticator (apart from for Jisc staff members). Even if the organisation with which the individual is associated is part of the Jisc community, the host organisation must be a member of eduroam(UK).

Is eduroam available to all members of an organisation?

To whom the member organisation grants a network access account and to authenticate is a matter for the organisation to decide, provided that the various Janet AUP and Security policies are complied with and that the private network status of Janet is not compromised; this results in the exclusion of general members of the public and alumni who are not currently actively engaged with the organisation/university. Temporary visitors such as conference delegates and people engaged in joint research with the organisation/university may be given network accounts strictly for the duration of their association with the university. This is all covered in the documents under https://community.jisc.ac.uk/library/janet-policies/eligibility-policy-guidance [6]

All members of organisations whose primary business activity is research or education are eligible to be given credentials for eduroam roaming.

Organisations whose primary activity is not research or education, but who are nevertheless eligible to participate in eduroam(UK) (e.g. local authorities, national health service organisations and other public sector bodies - see separate FAQ) as a Home service (IdP) provider, must limit eduroam roaming capability to those members who are engaged in research, education, training or support of these activities.

Can alumni be granted eduroam accounts?

The Janet AUP, Security Policy and the private network status of Janet result in alumni generally being ineligible to be granted network access privileges and hence eduroam enabled accounts. Together with former members of staff, alumni may only be given eduroam credentials if they have an ongoing close association with / are currently actively engaged with the organisation/university / are on site for the purpose of contributing to the organisation's primary business activity (research/education).

The network accounts of students/researchers/staff who have left the organisation and no longer have a close association should be promptly disabled, as least in respect of eduroam and the leavers should be encouraged to delete the eduroam profiles from their devices.

Do users need to have a network logon account?

Yes, users need to be authenticated by their host organisation. Such authentication is for the purpose of providing eduroam network access. Most organisations deploying eduroam make eduroam their primary network. It would be permissible for a user to have an eduroam account that the organisation did not permit local network connectivity for - although we can't think why. A more understandable scenario would be where a small organisation did not
provide its own eduroam Wi-Fi service but still acted as an eduroam IdP, for instance an organisation that is hosted by/embedded in a university/NHS trust/local authority.

**What about access for the public/non-registered users?**

To whom the member organisation grants a network access account and to authenticate is a matter for the organisation to decide. Such users will invariably need to register to be granted a network access account. Organisations may grant temporary accounts for visitors to conferences, events, training courses, contractors etc. provided that the various Janet AUP and Security policies are complied with and that the private network status of Janet is not compromised. Unregistered access for the public is not permitted - see the Janet factsheet on Guest and Public Network Access https://community.jisc.ac.uk/library/janet-policies/guest-and-public-network-access [7]

**Can we have an additional top level realm for our organisation?**

Yes, provided that your organisation is entitled to use the DNS domain. The technical wording is 'owns or manages by delegation'. We interpret this to include realm names/sub-realms that the organisation owning the DNS domain has given permission for your organisation to use for eduroam. To request an additional top level realm, simple put in a request via the Jisc Service Desk / Jisc online service request form.

**Can sub-realms be configured for an organisation?**

Yes. This is a self service function that sys admins an perform via the eduroam(UK) Support server portal.

**4) RADIUS server configuration**

In this section you will find specific information on Radiator, FreeRADIUS and MS Internet Authentication Service / Network Policy Server as well as information relevant to all RADIUS software.

**Do you have links to the various RADIUS server platform websites?**

FreeRadius website [8]

Radiator website [9]

Microsoft IAS (Internet Authentication Service) (Windows Server 2003) website [10]


Cisco ACS (Secure Access Control Server for Windows) website [12]

Juniper Funk Steel-Belted Radius website [13]

**How many RADIUS client devices can my ORPS support?**

Please note that this answer relates to RADIUS clients (eg NAS devices - such as wireless access points and switches) NOT actual users using the ORPS.

FreeRADIUS - as many as your server can logically handle

RADIATOR - as many as your server can logically handle

CiscoACS - Number of Access Points. To determine the number of access points that a Cisco Secure ACS can manage, start with the assumption that each access point manages about ten WLAN users. Then divide the total number of users that can be supported by a Cisco Secure ACS - 21,000 by this number. With this formula we have 21,000 divided by 10 or 2,100 access points that can be supported by one Cisco Secure ACS. This is the minimum number of access points that can be supported because not all access points will be supporting the maximum number of users at any one time.

Number of Network Access Servers - a Cisco Secure ACS can support up 5,000 discrete network access servers (NASs). This number can be increased by the use of the multi-NAS capability of an ACS. Multi-NAS is a concept that allows one or more addresses to be configured for a given NAS entry. Using multi-NAS, the Cisco Secure ACS can support a theoretical maximum of 255 multiplied by 5,000 discrete NAS equaling 1.275 million devices. However, a configuration of 1.275 million devices per Cisco Secure ACS is clearly not realistic.

What RADIUS server software are eduroam participants using?

Number of ORPS installations by RADIUS software type:

<table>
<thead>
<tr>
<th>Number of ORPS installations by RADIUS software type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>FreeRADIUS</td>
</tr>
<tr>
<td>Microsoft IAS/NPS</td>
</tr>
<tr>
<td>Radiator</td>
</tr>
<tr>
<td>Cisco Secure ACS</td>
</tr>
<tr>
<td>Cisco IOS</td>
</tr>
<tr>
<td>Aruba Clearpass</td>
</tr>
</tbody>
</table>
Are there any known issues with certain versions of RADIUS server software?

Yes! We of course make the general recommendation that you keep your RADIUS server software updated to the latest releases. There are particular known issues with versions of the popular choices of RADIUS software, including the following:

**FreeRADIUS** - versions prior to 1.1.4 do not support Vista clients due to the change in PEAP handling with Vista compared to XP. 1.1.5 and 1.1.6 had further SSL fixes to improve/fix SSL behaviour and stability in general...as well as more than 30 other bug fixes.

Versions 1.1.3-1.1.7 are vulnerable to being crashed by an attacker sending a Tunnel-Password attribute in an Access-Request packet.

If you are sticking with 1.1.x code, 1.1.8 was the final version of the 1.1.x product.
However we see no reason not to upgrade to the 2.1.x version of FreeRADIUS. 2.1.7 is at the time of writing the latest release and fixes many 1.1.x issues.

Further details regarding security vulnerabilities of FreeRADIUS versions can be found here: http://freeradius.org/security.html [15]

**Radiator** - in June 2007 the eduroam(UK) NRPS had to be upgraded to the current version due to several EAP-TLS broken parts. This was leading to failed authentication attempts from visited sites for users from a participating organisation using EAP-TLS with MS IAS.

The problem, which was traced to the RADIUS exchange not completing, was resolved by upgrading our NRPS Radiator software from v 3.13 to 3.17.1. It is likely that if you are running older versions of Radiator on your ORPS and you get a visitor from a site that utilises EAP-TLS then similar problems will be encountered.

We specifically recommend that if you are still running older versions of Radiator, you should upgrade as soon as possible to the latest version. (Radiator 4.4 is the latest version, last modified 11 March 2009).

In addition to the above, a compounding problem was that the ipf firewall software configurations on our NRPS were set to discard UDP fragments. The script was therefore changed to pass fragments using the keep frag keyword. If you employ the ipf filewall on your ORPS, you should check this.

A full history of Radiator software revisions can be found here: Radiator Revision History [16]

**Are there any example configurations for Radiator available?**

We currently don't have any direct cut'n'paste for Radiator that is clearly available for any site due to the uniqueness of each site requirement (backend authentication and such).

However, OSC (the publisher of Radiator) has produced a number of example configuration file snippets and templates which can be found in the goodies directory on a Radiator server. Eg. ntlm_eap_multi.cfg is a simple config which handles Radius PAP, CHAP, MSCHAP and MSCHAPV2 and also handles the outer and inner requests for TTLS and PEAP. In this case, the <AuthBy NTLM> sub-handler is doing the work. (Of course this is only suitable for Active Directory. If sites are using passwords or eDirectory etc then the requirements will be different).

**Resources:**

Also appendix A.2 of the Geant2 Roaming Infrastructure Service and Support Cookbook [17] provides useful information on configuring the ORPS server software.

**Are there any example configurations for FreeRADIUS available?**

We don't have any direct cut'n'paste configurations for FreeRADIUS that would be suitable for all sites due to the uniqueness of each site requirement (backend authentication etc).

However there are some hints and tips on the Support web site and there is some useful information in the following case study, which is a practical description of how University of Bristol implemented and complies with the Technical Specification using FreeRADIUS in an
AD environment: A Case Study in Complying with the Technical Specification.

- Also appendix A.2 of the Geant2 Roaming Infrastructure Service and Support Cookbook [17] provides Roaming Technology - FAQs useful information on configuring the ORPS server software.
- FreeRadius website [8]

What is unlang?

The unlang language available in FreeRADIUS takes flexibility in authorization to new heights. Unlang is not a full blown programming language, but rather a processing language. The purpose of unlang is to implement policies and not to replace complex scripts like those created with Perl or Python. Unlang sticks to a basic syntax that includes conditional statements and manipulation of variables. The unlang code does not get compiled but is interpreted by the FreeRADIUS server. The interpretation happens when the server reads the configuration files, which typically happens during start-up. The use of unlang is restricted to specified sections inside the configuration files and cannot be used inside the modules.

Source: https://www.safaribooksonline.com/library/view/freeradius-beginners-guid... [18]

Where can I get up to date binaries for FR2.2 for Centos (which ships with an old version)?

As of Jan 2015 CentOS 6.5 ships with 2.1.12, which is a somewhat deprecated version. I'm keen to get an up to date version. I'm loathe to compile from sources because we don't have the time to maintain manually compiled versions of things.

Try here:
http://software.opensuse.org/download.html?project=home%3Af reeradius%3A2.x.x%3Acentos&package=f reeradius [19]

What's the Difference between MS IAS and NPS?

Here's what msdn says - Internet Authentication Service vs Network Policy Server [20]. But we have also found difference in that IAS requires a workaround to be applied in order to avoid a problem related to Operator-Name

Microsoft IAS Deployment

- Basic IAS Installation and Configuration [21] (TechRepublic paper 2007)
- Microsoft IAS (Technet) [10]
- Deployment of 802.1X for Wired Networks Using Microsoft Windows [22]
- Deploying MS IAS with VLANs [23]
- MS IAS Operations Guide [24]

Microsoft NPS (Windows 2008/R2 and 2012/R2) Deployment

- 802.1X Authenticated Wireless Access (Technet) [25] - contains Design and Deployment guide sub-sections
- Complete How to Configure Microsoft NPS (Technet) [26] - deployment as RADIUS authentication and RADIAS proxy server
Troubleshooting Microsoft IAS as a RADIUS server and as a RADIUS proxy

This link to the MS TechNet site should be useful:

- IAS Troubleshooting as a RADIUS server - Authentication Problems (Technet) [27]
- IAS Troubleshooting as a Proxy server - RADIUS Forwarding Problems (Technet) [28]

Our AD usernames don't match eduroam username format, how can I strip/modify realm for authentication?

Our usernames in AD just use the userID format not userID@realm [29] - how do I strip the realm prior to authentication?

Our usernames in AD use a different realm (e.g. @ad.camford.ac.uk) - how do I modify the realm component?

The recommended solution is to add the required realm as a UPN in AD - this will allow NPS to authenticate the eduroam usernames against your AD.


Cisco ACS Implementation

We have configured the relevant databases for our ACS servers and ports on the ASA firewalls, now we need some help in configuring ACS 4.0 for PEAP.

The following Cisco links give various bits of help regarding ACS and PEAP:

- PEAP under Unified Wireless Networks with ACS 4.0 and Windows 2003 [31]
- System Configuration: Authentication and Certificates [32]

When initially setting this up it is a good idea to maximise the logging as follows.

How to Set the Logging Level to Full in the ACS GUI:

You will need to set ACS to log all messages. To do this, follow the steps listed below:

1. From the ACS home page, go to Systems Configuration > Service Control.
2. Under the Service Log File Configuration heading, set the level of detail to Full.

You can also use the command line tools to further debug - there's a whole suite of them.

ACS Internal Architecture - CSTacacs and CSRadius [33]

CSRadius appears to be the most useful - for an example of it in action see:

Obtaining vs and AAA debug info for Cisco Secure ACS - RADIUS success authentication [34]

I've set up Attribute filtering - what Attributes should I NOT filter out?
The following is the minimum set of attributes required to support eduroam. These must not be filtered out:

RADIUS Access-Request or Access-Challenge message attributes:

1. User-Name
18. Reply-Message
24. State
25. Class
31. Calling-Station-ID
33. Proxy-State
79. EAP-Message
80. Message-Authenticator
   MS-MPPE-Send-Key
   MS-MPPE-Recv-Key
89. Chargeable-User-Identity
126. Operator-Name

RADIUS Accounting messages:

1. User-Name
25. Class
33. Proxy-State
40. Acct-Status-Type
44. Acct-Session-ID

This list has been determined following a small number of incidents involving Roaming users being unable to connect at certain institutions (both here in the UK and elsewhere) owing to over-restrictive attribute filtering. Please note that implementation of the list is likely to become a mandatory feature of eduroam.

If you are aware of any other attributes then please contact eduroam Support.

For more information on this topic see:

- List of RADIUS Attributes [35]
- RADIUS Attributes [36]
- Attribute Screening for Access Requests on Cisco Network Access Server [37]

**What procedure do I need to follow for changing the IP address of our ORPS?**

You need simply to use the https://support.eduroam.uk [38] support site. Go to your ORPS configuration page and select your ORPS, change the name of the RADIUS server and press [Update RPS]. Check that the passphrase does not change (it should not). The final step is to remove the old ORPS entry and add the new one. The passphrase will be different then. The changes are propagated to the NRPS on the hour.

**How do I set the shared secret for ORPS in a fail-over cluster to be the same?**

It is best practice to use one shared secret for each ORPS-internal RADIUS server pair. This is to limit the effect of one RADIUS server being compromised or having the credentials
leaked giving further access to the rest of the RADIUS infrastructure. In some cases it is not feasible to have separate shared secrets, for example in a system where the RADIUS servers have a shared/synchronised database.

In this case you can request eduroam(UK) Support to set the same set of shared secrets to be same for all you ORPSs.

**IP Addresses/FQDNs/shared secrets for ORPS - replacing ORPS and moving to a new location**

**What is the recommendation regarding use of same or unique shared secrets for ORPS/ internal RADIUS servers?**

*We have multiple internal RADIUS servers at departments and colleges, should be use separate shared secrets for each pairing or would a common one be acceptable?*

It is best practice to use one shared secret for each ORPS-internal RADIUS server pair. This is to limit the effect of one RADIUS server being compromised or having the credentials leaked giving further access to the rest of the RADIUS infrastructure. In some cases it is not feasible to have separate shared secrets, for example in a system where the RADIUS servers have a shared/synchronised database.

In this case you can request eduroam(UK) Support to set the same set of shared secrets to be same for all you ORPSs.

We don’t think our ORPS are communicating with the NRPS properly although we’ve set the NRPS up as clients and configured forwarding. What’s going wrong?

*Invalid message authenticator’ error entries as below are being seen in the NRPS error logs views on eduroam(UK) Support:*


and

**Mon Oct xx xx:xx:xx 2014: WARNING: Bad authenticator in request from xxx.yy.zzz.118 (xxx.yy.zzz.72))**

Bad authenticator in an Access-Request indicates that the shared secret is incorrect. So the log error entry indicates that an ORPS that has a incorrect shared secret configured for a NRPS. (Remember, each NRPS-ORPS pair has an individual shared secret).

If there is a further IP address in brackets in the error entry, this indicates that you might have an internal system with an incorrect shared secret with your ORPS. (Best practice is for each RADIUS pair on your internal network to have its own secrets). The NAS systems (APs, WLCs [switches if applicable], that talk to your ORPS internally need to have their own correct shared secrets. If your ORPS behaves badly and forwards RADIUS packets containing a bad EAP Message-Authenticator, the result will be that the NRPS detects the error, drops the packet and records the entry in the log - which is propagated to your view of the error log on eduroam(UK) Support.
Solution - correct your shared secrets on NASs and ORPS.

'Unknown client' error entries are being seen in the NRPS error logs views on eduroam(UK) Support:

Unknown client means that the RADIUS client is unknown, the NRPS don't recognise the IP address of the RADIUS server that is sending authentication requests to them. This could be because you have not correctly added the ORPS details into the ORPS config screen on the Support server. Alternatively it could be that there is a DNS issue. You define your ORPS as a FQDN. If this is not correctly resolved or if your ORPS is using an address other than can be resolved, the NRPS will not reply and the unknown client error will be logged.

Does Microsoft NPS support RADIUS accounting and how to avoid forwarding accounting packets to NRPS?


By default NPS does NOT forward accounting packets, but it is possible to configure the server to do so!

Microsoft documentation states: ?Connection request policy accounting settings function independently of the accounting configuration of the local NPS server. In other words, if you configure the local NPS server to log RADIUS accounting information to a local file or to a Microsoft® SQL Server? database, it will do so regardless of whether you configure a connection request policy to forward accounting messages to a remote RADIUS server group.?

To comply with eduroam(UK) Tech Spec you need to ensure that you configure the local NPS server to log RADIUS accounting information to a local file or to a Microsoft® SQL Server? database.

The May 2016 eduroam(UK) advisory notice requests that you ensure that you have NOT set a connection request policy to forward accounting messages to the NRPSs.

NB. A default connection request policy is created when you install NPS. This policy has the following configuration:

- **Authentication** is not configured.
- **Accounting** is not configured to forward accounting information to a remote RADIUS server group.
- **Attribute** is not configured with attribute manipulation rules that forward connection requests to remote RADIUS server groups.
- **Forwarding Request** is configured so that connection requests are authenticated and authorized on the local NPS server.
- **Advanced** attributes are not configured.
To learn about accounting and logging in NPS see:

https://technet.microsoft.com/en-us/library/dd197475%28v=ws.10%29.aspx [40]

Further references:

https://technet.microsoft.com/en-us/library/dd197475%28v=ws.10%29.aspx [40]

5) Server Certificates for ORPS

Can I use a self-signed certificate for my RADIUS server?

Yes. The RADIUS server certificates required by certain EAP methods may be derived from a self-signed certificate authority (CA) / private certificate authority or they can be purchased from a commercial public CA.

EAP methods that use transport layer security (TLS), such as EAP-TLS, EAP-PEAP and EAP-TTLS, require the use of a server certificate to authenticate the RADIUS server to the supplicants. In addition EAP-TLS requires client certificates too in order for the clients to be validated by the RADIUS servers. These client certificates can be self-signed, i.e. generated by your private CA software.

The advantages and drawbacks of both using private and public CAs are listed below.

Using a certificate from a self-signed private CA

Benefits:

- No need to purchase a certificate from a commercial vendor - saving cost.
- Provides a slight security benefit by making it harder for a user to misconfigure their supplicant in an insecure way. (The use of a certificate from a commercial CA combined with a failure by the supplicant to validate the CN of the certificate makes a MITM attack feasible, where the attacker simply acquires a certificate from the same CA).

Drawback:

- You will generally have to install or get the laptop user to install the server ?root certificate? from your self-signed Certificate Authority on each client before it will recognise a private server certificate - but this is not a difficult procedure.

Using a certificate from a commercial CA
Benefits:

- No need to distribute the CA’s root certificate to each client since public CA certificate will generally be recognised by any client, since such certs are distributed with operating systems.
- The correct extension attributes will be present (if requested or needed) - eliminating necessity of configuring openssl etc.

Drawback:

- Cost - you usually have to pay an annual fee for each certificate.
- Slight vulnerability to illegal spoofing

Note: some RADIUS implementations, such as Radiator and FreeRADIUS, provide a certificate from a self-signed CA for testing purposes. Under no circumstances should this certificate be used in a production environment.

Resources:

- TechRepublic paper (2007) - Self-sign a RADIUS server for secure PEAP or EAP-TTLS authentication
- Microsoft technical article - Certificate requirements when Using EAP-TLS or PEAP with EAP-TLS
- Private certificate authority software

Can I use the Jisc Certificate Service to provide certificates for my RADIUS servers? / Do you have any technical documentation on using MS IAS and Jisc Cert Service?

Yes - the Jisc Certificate Service works fine with the most popular RADIUS servers; FreeRADIUS, Radiator and Cisco ACS and will provide you with server certificates free of charge - suitable for use with EAP-PEAP and EAP-TTLS methods. However if you intend to use Microsoft Internet Authentication Service (IAS) with Jisc SCS, skilful configuration will be required. A draft guidance tech guide sheet is available on request.

The difficulties with MS Internet Authentication Service stem from the fact that it does not send the full certificate chain during EAP-PEAP negotiation. Consequently, in order to use IAS with Jisc SCS certificates (or any other certificate not issued directly from a certification authority (CA) ‘known’ by the supplicant), it is essential to:

1. Ensure that you include the correct extensions in the certificate
2. Configure IAS to include the certificate in its list of known certificates.

This issue came to light through problems experienced in attempting to use certificates issued by the Jisc SCS with the Windows XP supplicant. All certificates issued by the Jisc SCS are signed as from an intermediate CA; but any 802.1x supplicant, including the one native to XP, will not be able to validate certificate chains derived from intermediate CAs from Microsoft IAS because IAS does not send the full chain in the ServerHello during the TLS handshake in Phase 1 of EAP-PEAP.
So if you intend to use Microsoft IAS, your options are:

1. Choose a vendor that will supply a certificate that will 'chain directly' to a root CA 'known' by your supplicants.

2. Be very careful and thorough in your configuration of IAS.

[Anyone considering use of Jisc SCS certificates should read the Janet guide - Using Certificates Issued by the Jisc SCS with MS IAS.]

3. Manage your own private CA.

**What do we need to configure on client workstations in order to use the TERENA certificates supplied through the Janet/Jisc Certificate Service?**

DRAFT ANSWER!

Windows (and other OSs) only natively trust certain certificate CAs for 802.1X. The certificates provided by Jisc used to be supplied by Comodo (UTNAddTrustServer_CA, TERENASSLCA and AddTrustExternalCARoot) but are now supplied by QuoVadis.

Is there a way around this without the end user having to configure their advanced wireless settings?

Old Comodo certificates supplied through TERENA under the Jane/Jisc Certificate Service:

USER Trust - UTN-USERFirst-Hardware-TERENA SSL CA

AddTrust External CA Root is in the Windows default list. Have you ticked this CA in the list of Trusted Root Certification Authorities in the PEAP properties.

The Jisc Certificate Service now (April 2015) of course provides QuoVadis certificates and you need to use the appropriate CA as the Trusted Root Certification Authority.

**Can I use the same certificate for more than one ORPS?**

Yes you can indeed use the the same certificate for more than one ORPS. In fact it's better to do this because then there is only one CN for the client to be configured with.

**How do I get and install a commercial server certificate for use with MS IAS?**

MS IAS - obtaining and installing a VeriSign WLAN Server Certificate for EAP-PEAP (MSCHAPv2) [47]

**Are there any likely issues for users when we replace our JCS-supplied ORPS server certificate?**
Our ORPS server certificate is due to expire shortly and we have a replacement JCS certificate which uses the identical three intermediate certificates in our old certificate (Addtrust, UTN and Terena CA). Users have been using eduroam profiles created using the cat.eduroam.org installer. The question is: Will there be any impact on users if the latest radius certificate is applied on our end (authentication) servers?

There shouldn't be any issues if users have configured their device correctly to trust the CA and only the CN of the ORPS server. By contrast, clients in which the set up process has been shortcut by just entering username and password after clicking on 'connect to eduroam' will have problems. This is because devices often install the RADIUS server cert and trust only that certificate when the user just clicks on the SSID and enters their username and password.

Our ORPS server certificate is about to expire, what do we do?

If the new certificate is just a renewed version of the old one, signed by the same root CA then the trust installed on end user devices will still work and all you need to do is replace the old certificate file with the new one. See http://docplayer.net/13268335-Server-certificate-practices-in-eduroam.html [48]

If you are using a new CA, or the CA has changed its root certificate in the mean time, you will need to update the root CA installed with the eduroam profile in end user devices. For most devices you can install a second root CA in the profile in advance so it doesn't need to happen on switch date all at once. Some android devices don't have support for multiple roots in a profile so these will need to be updated after the switch. See the 'CA rollover support' section in https://wiki.geant.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+institution+administrators [49] and https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations [50]

6) Integration of RADIUS Server with Back-end User Database

Is it possible to authenticate EAP-PEAP against Novell Directory Services?

While it is not possible to authenticate EAP-PEAP against the default non-reversible hash used in NDS, it is now possible to configure a "Universal Password" in NDS which stores users' passwords in a reversibly encrypted format. This will permit the authentication of EAP-PEAP against NDS through RADIUS servers such as FreeRADIUS and Radiator.

How do you configure FreeRADIUS against Novell eDirectory?

Novell has produced documentation on configuring FreeRADIUS against eDirectory:

http://www.novell.com/documentation/edir_radius/index.html [51]

FreeRADIUS integration with Active Directory

The received way of setting up FreeRADIUS to authenticate users against Active Directory is to use Samba/winbind/ntlm_auth:

FreeRADIUS Active Directory Integration Howto - from FreeRADIUS Wiki [52] (Login required)

University of Bristol implemented FreeRADIUS in an AD environment. The following case
study contains useful information: A Case Study in Complying with the Technical Specification.

**Radiator integration with Active Directory**

The first thing to note is that different handlers in the radius.cfg should be used dependent on the OS platform of your Radiator server. AD is also problematic as it will not permit access to plaintext password by the RADIUS server.

There are a large number of sample configuration files and templates in the 'goodies' directory on Radiator servers which should prove helpful. These can be modified to suit your environment with options configured such as domain name, IP address, password etc.

**Realm name not in AD - can we get NPS to translate realm?**

You cannot manipulate the realm with NPS - this is something that you used to be able to do in the IAS days, but on all modern clients it will cause EAP to fail because the MPPE key derivation is from the original client-provided username, not from what a RADIUS server might turn it into. You shouldn't be attempting to manipulate the realm though - if AD is your backend then you actually just need to add the realm in question to the AD as another global UPN - NPS in AD will then just handle it.

You can read more here: https://social.technet.microsoft.com/Forums/windowsserver/en-US/e73183d4-7b2f-48a7-9246-97ed711e8e8d/eappeapmschapv2-realm-stripping?forum=winserverNAP [53]

7) **Authentication Issues**

Is 'machine authentication' permitted a) for roaming users b) for devices that will only connect on campus/at corporate office?

a) No, machine-based authentication (using usernames in the form 'domain\hostdevice') for machines roaming away from your own campus via eduroam is not permitted. eduroam policy states that the username needs to be in NAI format - ie userID@realm [29]. 'Machine authentication' is usually based on the utilisation of non-RADIUS-routable usernames in the form 'domain\hostdevice' so use of this format of credential is not possible technically in any case. eduroam policy requires that roaming authentications are based on the authentication of an individual identifiable and traceable user. If credentials such as deviceID@realm [54] (e.g. with a cached password) were to be used, whilst RADIUS-routing is possible, the user of the device could not be verified (note that secondary authentication is not permitted nor supported in eduroam) and it would not be possible to track down any individuals using the machine should there be a breach of Janet security policy. Hence machine-based authentication using credentials such as deviceID@realm [54] is not permitted when roaming.

b) However for devices that will only connect on campus/at corporate office, yes you may do machine auth on your own campus - with the proviso that you have the means to track down any individuals using the machine should there be a breach of Janet security policy. In practice this means that a device you want to machine-authenticate should be assigned to a responsible user. Such machines will not normally have RADIUS-routable usernames (since they will be in the form 'domain\hostdevice') and you must not try to create RADIUS-routable credentials for machines - although technically certificates could be issued in order to identify devices with a username 'device@realm [55]'. 

Can we utilise generic eduroam accounts for corporate devices we issue to registered staff/post-grads/students where we record which device is issued to which user?

Logging of user connection/activity would still be identifiable because the MAC address of the device issued to each individual would be recorded in our library management system.

eduroam(UK) policy requires that the spirit of the Janet Security and AUP are complied and moreover use of the Janet network and connection to it require adherence to those policies. eduroam logging policy requires that the individual is traceable if necessary, so the use of uniquely assigned credentials and logging of connection event time, IP address, MAC address and user credentials are in general the logging requirements. If generic credentials are used, the individual can still be identified through the MAC address-user record (although MAC addresses can be spoofed). It is therefore acceptable for generic credentials to be used in the above scenario.

How can I differentiate between Institution-owned/managed devices and user-owned devices, (I want to manage the network environment they connect to after user authentication)?

One method to identify which auth requests come from institution-owned devices is to use the wireless MAC address of the device, which is included in the Calling-Station-Identity attribute in the Access-Request. Then to manage the network environment the authenticated user's device is connected to, do dynamic VLAN assignment.

Devices with MAC addresses known to belong to institution-owned/managed devices could be connected to your corporate network and unknown ones could be connected to your BYOD (insecure network for home-organisation users). Authenticated visitors should of course be placed onto your proper eduroam VLAN network. All of the above can be achieved through a single 'eduroam' SSID.

MAC addresses of course can be spoofed, so this is not method cannot be guaranteed to be 100% secure.

Another method would be use a certificate-based authentication mechanism, ie EAP-TLS. By setting certain parameters in the client certificates issued to institution-owned devices, your ORPS can be made aware of the category of device and return the relevant attribute to result in the device being connected to the required VLAN on your network.

When network passwords are changed the cached credentials on user devices have to be manually updated which sometimes creates issues for users

If using a password-based mechanism this is typically the case. Clients are dumb and some won't understand why an authentication request has failed after a central password change. However, there are ways of sending a request from the RADIUS server if the password is incorrect to make the client re-prompt the user for a password - that's IF the client supports such a prompt and the RADIUS server supports the mechanism.

Can't get Visited service to work - NRPS do not appear to be responding at all/ignoring all our ORPS/blocking auth requests
There are two cases when the NRPS don't respond to requests:

1) the server contacting them is not registered

2) the ORPS is registered but the shared secret is incorrect

Incorrect shared secrets are always logged as errors on Support Server and you will see these in the RADIUS errors log on the Troubleshoot page. With unregistered hosts it can be difficult to know which organisation they belong to so if your RADIUS server is not registered in Support you will only see them in your logs on the Support Server IF we can pick up enough info from the rDNS and WHOIS records.

Note that firewall issues may also result in the symptom that the 'NRPS are not responding'

If only some auth requests are ignored, this indicates either that the visitor's home ORPS is not responding or the authentication request contains an valid realm name.

8) eduroam Policy Related Issues and Dealing with Virus/Copyright Breach Incidents

Can you clarify Jisc's eduroam(UK) Policy/Tech Spec on visitor logging?

Clarification of eduroam Policy and Tech Spec Wording - Visitor Activity Logging.

In cases of major abuse by visiting guest eduroam users, who should we contact?

(By major abuse we mean those about which we receive a complaint from an outside organisation).

Fortunately such cases are few and far between, however if you receive a complaint from an outside organisation about a guest user on your network (eg. illegal copyright download notice), the user's Home organisation should be contacted immediately.

In the first instance you should try to contact the eduroam technical administrator at the Home site AND also please copy in Jisc Service Desk quoting 'eduroam' in the subject line. Contacts are listed on the eduroam Support Server General Information page. If you have difficulties in tracking down the administrator at the Home site (eg. in cases of visitors from outside the UK where searching on the eduroam.org site has been unfruitful), please contact Jisc Service Desk and we will pursue the matter with eduroam.

Say we receive notification from Jisc CSIRT about suspected virus activity giving an IP address which turns out to be used by an eduroam visitor at our site, what do we do about it?

So CSIRT detects virus-related activity coming from your visited site and notifies you giving the IP address of the offender (who may be an eduroam user) and the date/time of the incident. You need to determine the MAC address and probable home organisation of the offender using your detailed DHCP and RADIUS logs and you should then contact the home organisation to report the incident.

Obtaining MAC address and probable home organisation details:

Given the IP address CSIRT provides, your DHCP log should reveal the MAC address of the
offender. The RADIUS log includes user-name, acct-session-id and calling-station-id attributes. Again, by using the IP address, the MAC address should be evident from the calling-station-id attribute and this should match the address revealed from the DHCP log.

You will be able to provide the probable realm name of the offender (from the user-name record, which can only be used to determine realm since the visited site RADIUS log only shows details of the outer ID/stage 1 authentication of an EAP authentication - which will be null@usersiterealmname.ac.uk [58] or anonymous@usersiterealmname.ac.uk [59] or realfred@usersiterealmname.ac.uk [60] in case of WindowsXP and Vista supplicants. Only the inner ID/stage 2 authentication utilises the real user ID). Nb. we cannot be certain that the indicated realm name is a definitive pointer to the realm of the real user ID since due to erroneous set up of proxying by some sites, the inner ID may be proxied off to another organisation for final authentication (we run a scan once a month to expose such errors).

Action:

The probable home site should now be contacted for details about who that user was (using date and time stamp details from the visited site logs, the home site should be able to track down the user and deal with the incident). The eduroam technical contacts/site eduroam administrators are listed here: https://support.roaming.ja.net/?q=general [57]

What should we do if we identify a virus infection on a visiting user?s laptop if they are still on our eduroam guest network - do we have the right to block their access (based for example on MAC address of the Calling-Station-ID) or do we report this to eduroam Support (which will then escalate to the Home institution to deny authentication)?

If a visitor has a device with a proven virus infection or they breach yours or the Janet AUP then you should indeed block their access to your guest network. As service provider, you are certainly have the right to block access. You should however have a mechanism by which they know that they have been blocked for that reason - eg some captive page or network walled garden that gives them that information.

The case must also be escalated to the Home institution AND eduroam Support. Note that the visitor could be from a non-UK organisation so by notifying eduroam Support the issue will be pursued with eduroam.

Also note that whilst blocking MAC address is a simple method of denying access it could be circumvented if the visiting host is intent on more malicious activity (likewise, blocking on outerid won?t be effective either).

9) RADIUS Server log Keeping and interpreting Errors in the ORPS logs

Keeping RADIUS logs is a requirement of the Technical Specification and we strongly recommend routine inspection of the RADIUS logs in order to reveal any underlying issues that may not be causing an obvious degradation of the service, but which will nevertheless be having an adverse effect on performance.

Generation of Monthly Stats on eduroam usage for Microsoft IAS/NPS
We’ve been asked to provide monthly stats on the number of internal and external users of our eduroam service, which is built on MS NPS. Is there an easy means of doing this?

Analysing/filtering the log files on the NPS servers is proving difficult since these are used for authentication by multiple SSIDs).

You will need to either parse logs or configure your ORPS/RADIUS server to log to a dB or file. If your system cannot log auth accept/fails to a separate simple log or an external dB then parsing of its internal/local log will be your only option. There is a Microsoft TechNet article which addresses this: http://technet.microsoft.com/en-us/library/dd197475(WS.10).aspx [61]

Microsoft NPS Error 'RADIUS Client Authentication Attribute not Valid' (ID 18) appearing in our logs. What is causing this?

This error message indicates an incorrect shared secret. To fix this look at which RADIUS client (AP / Controller / RADIUS Proxy etc) is causing the error and check the match of the shared secret. Remember that, unless specifically requested otherwise, there is a different shared secret for each ORPS-NRPS combination. Also, the RADIUS client related to the issue may be one of your own RADIUS clients on your network - if you only have one ORPS and the automated JRS authentication monitor shows access-accept for the test account at your realm via all three NRPS, this indicates the shared secrets with the NRPS are fine. Microsoft TechNet article on this: Access-request message received with authenticator attribute not valid. [62]

Microsoft NPS Error 'Wrong Domain' (ID 4402) appearing in our logs. What is causing this?

This error indicates that a domain controller can't be found for an authentication request from one of your RADIUS clients. You are receiving a request, which you aren't forwarding to the NRPS, but there's no domain controller available to handle the request. To investigate further you need more details about the error instances, i.e. for which domain a controller cannot be found. Microsoft TechNet article on this: There is no domain controller available for domain. [63]

Peaks of re-authentications at certain times of the day/heavy auth load leading to failures and poor performance

We use FreeRADIUS and AD and are experiencing issues at particular times of the day when our re-authentications appear to be increasing in frequency causing a large amount of failures. This is resulting in the eduroam(UK) Nagios check also being affected. What can we do to rectify this?

This is most likely to be due to slow responses from your AD when performing NTLM auth. It is a problem which affects all large institutions and there are different approaches to fix this. Some universities we have moved to using EAP-TLS as the primary authentication method, which doesn’t require an AD auth. However, then you need a system to manage the client certificates. (E.g. Cloudpath ES but there are others.)

Some organisations, have moved to Samba 4 and tweaked the settings to improve performance. See the NWS 43 presentation on this subject.
Some quick fixes are to increase the MaxConcurrentApi setting on the Domain Controllers
https://support.microsoft.com/en-us/kb/2688798

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/faqs-eduroam-system-administrators-and-implementation-techs

Links
[29] mailto:userID@realm