FAQs for eduroam System Administrators and Implementation Techs - Part 3

10) Wireless Networks

- How many SSIDs should be implement?
- Solving/mitigating the 'Overlapping eduroam Visitor service Problem' (aka the 'Russell Square' Problem)
- Do we have to support eduroam on 2.4GHz?
- Hints for Multi-floor Wi-Fi deployments
- Wi-Fi Surveying - help identifying a company which can provide a survey service
- Must we broadcast eduroam SSID rather than having it as a hidden SSID?
- Do we have to deploy a RADIUS server; can't we just peer our WLC with the NRPSs?
- How do you configure a Cisco 1200 Series Wireless Access Point for eduroam SSID?
- Can Cisco fat WAPs be used with multiple broadcast SSIDs and dynamic VLANs?
- Convertion of 'fat' Cisco WAPs into 'thin' ones
- WPA2 / WPA fallback for clients and APs - archived content

11) Supporting Users

- What sort of support for the users to we need to provide?
- How do I get access to the eduroam CAT (Configuration Assistance Tool) web site?
- What do I need to do to get my federated access SSO service to support my sys admin access to CAT?

10) Wi-Fi Networks

Do we have to support eduroam on 2.4GHz?

No you do not have to support 2.4GHz eduroam. Indeed a 5GHz service could perform better in many situations. Have a look at the Optimize your WLANs for Phones and Tablets presentation (scroll to the near the bottom of the page) : https://www.jisc.ac.uk/events/wireless-mobility-event-27-feb-2019 [1]

For many organisations, for instance the NHS, where a lot of equipment is connected via Wi-Fi but much of the equipment only supports the 2.4G band, the case for providing eduroam in the 5G band (and future 6G band) is even stronger. This allows the 2.4G band to be dedicated to non-eduroam authenticated devices and avoids the need to advertise the eduroam SSID in the 2.4G band.

How many SSIDs should we implement?

The answer to this is entirely dependent on your needs and policy, but you should aim to keep the number as low as possible. Different areas of your campus will have different needs, so

you don't need to provide all SSIDs to all areas. (For instance a gaming/TV/audio device network for devices that do not support 802.1X could be limited to halls of residence).

The eduroam SSID is obviously a must-have for all or most areas of campus. This one SSID can serve the needs of many network users that pre-802.1X would have needed multiple SSIDs. By using dynamic VLAN assignment the one SSID eduroam can support many groups of users and devices (e.g. staff, students, eduroam guests, other, 'machines') that have very different security profiles and requirements to access network resources. So one SSID can satisfy the majority of your requirements.

Then you will probably want a setup/provisioning/remedial SSID (e.g. open, captive portal, access to installer utilities/CA certificate, OS patches).

In addition you may want an SSID for a non-eduroam guest service (e.g. for public access and with either a separate ISP feed or a tunnelled link through Janet to the contracted hot-spot service provider). But consider if eduroam Visitor Access, which provides for eduroam guest credentials for visitors - thereby enabling guests to connect to your eduroam service, could eliminate the need for or at least reduce the scale of expensive public access services. eVA is certainly very easy for host and admin staff to use and offers a wealth of options including SMS request self service guest accounts.

If you have halls of residence you may want an SSID for non-802.1X devices (e.g. multimedia devices, gaming, TV etc.).

http://www.revolutionwifi.net/revolutionwifi/p/ssid-overhead-calculator.html [2] useful for determining how many SSIDs you can handle. The old rule of thumb about no more than 4 SSIDs is based on broadcasting beacons at the old 802.11b 1Mbps rate. Consider whether you still need to support 802.11b. If you raise your minimum data rate you can handle far more SSIDs with the trade-off of losing client connectivity at the margins of AP coverage area. It could be argued that provision of a responsive service over a more limitied footprint (or one requiring a greater denisty of APs) is preferable to providing a poor data rate service that could lead to user dissatisfaction.

And you may need several SSIDs for WPA2-PSK services for specific purposes in specific limited locations. But consider implementing a single 'things' PSK wireless network.

How can we solve the overlapping eduroam service ('the Russell Square') problem? We would like to set up eduroam Wi-Fi but in a number of our buildings we get eduroam Wi-Fi from a neighbouring organisation. Some of our buildings are very close and the overlapping signal is very strong. We've been advised by our Wi-Fi supplier that any overlap would cause roaming issues for users. What are the possible solutions?

There are several solutions, however at the current time the best one is a technical method after political agreement (see below)

Technical method 1: use 802.11u (aka Hotspot 2.0/ HS20/passpoint) to identify the APs as being 'eduroam' but also belonging to your organisation. Compatible clients can then be configured to prefer the eduroam provided by your organisation. This is the ideal solution, however current client support is lacking (and when it is present it is fairly poor). The current eduroam position is decribed at:
https://wiki.geant.org/pages/viewpage.action?pageId=131634132 [3]

Technical method 2: conduct wireless surveys and liaise with your neighbouring organisation to ensure that wireless overlap is minimal, eg. turn down power of APs near the 'border zone' so that the correct APs are chosen by client devices when in the buildings in the overlap zone. This solution is complex and sometimes not possible due to wireless coverage patterns and required coverage areas from those bordering APs. This may also incurr additional cost due to the possible need to deploy additional APs to cover new dead spots and repositioning of APs.

Technical method 3 - don't provide the eduroam SSID where this service is provided through overlap from your neighbour - simply make use their eduroam wireless service in those areas. This obviously will mean that if you implement a single (eduroam) SSID network service with dynamic VLAN allocation for your own users, this will not be available at such locations. So you'll have a non-homogeneous/mixed service for your own users. Offsite (e.g. internet) resources will be accessible, but resources only available on a local user VLAN will be more difficult to access - although access could possibly be gained through a VPN. Visitors won't be affected, other than being unaware that the eduroam service they will be using will actually be being provided by your neighbour (potentially leading to support issues).

Political method - share layer2 VLANS between the 2 sites. You could feed your staff/student/visitor networks into each other's wireless domains and have RADIUS policy that states if the realm is that of your roaming L2 partner then allow agreed VLANs to be returned via their remote RADIUS server. For this to be viable you will need to have the transit mechanism, ie be neighbouring sites and connected to same NREN kit or have a direct link to your neighbour. This solution is the most satisfactory method for achieving inter-organisation roaming and ensures that when the staff/student/visitor client devices roam to the other location, they are still able to authenticate and drop onto the network as if they were on an AP in your own building.

This solution requires good, strong technical knowledge and the ability to share layer 2 networks between organisations (eg feed an 802.1Q trunk between sites). It needs to be done bilaterally (and can become very complicated when more than two organisations are involved) and with strict agreements/protection that you won't drop any other people onto such VLANS provided by you.

This is the preferred solution until hotspot2.0/802.11u becomes ubiquitous and method 1 becomes practicable (your wireless vendor's kit will need to support it and allow configuration of such beacon attributes).

Do have any advice on Wi-Fi deployment for multi-floor buildings?

To improve handling of a multi-floor situation, consider rotating the antennas 90 degrees so they provide a smaller horizontal footprint but penetrate multiple floors more effectively, and then stagger APs between floors (if you are wanting a single eduroam instance to span the

entire building), or you can dial down the power (or choose a cutting edge standard like 802.11ax that has less range) so that APs don't penetrate between floors at all (this would even facilitate separate eduroam instances on different floors to support different departments for which for instance you might want to implement different filtering policies for staff/your own FE students/HE students).

Hint: Dialling down the power of APs is as important and dialling up the power to ensure coverage. You would dial down the power to a) match the power *from* laptops/phones since it is essential the AP can receive signals from devices and not simply shout at them! b) you need to ensure a clear transition boundary between the converage cells of adjacent APs to help devices to associate with specific APS without having to continually re-scan - which is time consuming for the device.

This presentation contains further hints and tips and is well worth a read: Optimise your WLANs for smartphones and tablets [4]

Wi-Fi Surveying - help identifying a company which can provide a survey service

Jisc (and before that Janet) has never offered a wireless network survey service to identify where signals are weak / strong across the campus buildings to help establish where additional access points may be required and to inform Wi-Fi network design. That is very much a campus network related service and not something that we as an inter-institutional / internet network provider have got involved in.

If your organisation does not wish to carry out the Wi-Fi surveying/review of design yourselves, wireless network surveying is very much the domain of commercial networking companies. To identify a suitable supplier, the Jisc purchasing frameworks programme might be helpful to your organisatoin. The frameworks programme is described on https://www.jisc.ac.uk/frameworks [5] and the specific one that might be useful is https://www.jisc.ac.uk/network-equipment-framework [6]. 'It also covers converged network adapters, interface modules, transceivers, access points, voice over internet protocol (VoIP) products and associated ancillary goods and services including software, cabling and installation.' There is a drop down menu listing the suppliers who are in the programme.

You may find the Network Equipment Framework – Buyer's guide of interest: https://community.jisc.ac.uk/system/files/56564/Network%20Equipment%20-%20Buyers%20Guide%20v.6.pdf [7] (you'll need to request membership of the Community group to access that).

Is it essential for an institution to broadcast the eduroam SSID, as opposed to having it hidden? And would failure to broadcast eduroam mean an institution couldn't join eduroam?

Yes to both questions. Broadcasting the eduroam SSID is required by eduroam confederation policy and is an eduroam technical requirement. This is because firstly, it's a way of advertising the presence of the service. Secondly, the native WinXP SP2 supplicant cannot do 802.1x against a hidden SSID (see below).

Do we have to deploy a RADIUS server; can't we just peer our WLC with the NRPSs (particularly for Visited-only services)?

It would be technically possible to configure WLCs as clients of remote RADIUS servers - you

would need to allocate a public IP address for each WLC, create A records in your DNS and configure your firewall to support the addresses and forward to your WLCs. You would also need to set the WLCs as your 'ORPSs' in the eduroam(UK) Support server portal. However, this is strongly deprecated and there are further technical issues to be considered.

The deployment model on which eduroam is based is that of a RADIUS server being peered to the NRPSs with the member organisation's APs/WLCs providing the Wi-Fi service and pointed to the RADIUS server for authentication. The Technical Specification (to underpin the trust fabric of eduroam and to comply with security policies) requires that there is logging of authentication events. It also requires that non-essential VSA attributes, which in many cases essential to internal network operation, are not included in authentication responses to the NRPS/visited ORPSs - so it may be required that your system can support attribute filtering. In addition, some authentication filtering based on realm may be required. For all these reasons, unless your WLC system can support the aforegoing, the deployment of a RADIUS server is the strongly preferred solution.

Having a dedicated RADIUS server allows you to implement the following:

1. Choose a fully functional RADIUS server/service that meets your requirements/vendor supply policy (*)
2. Makes it easier to provision a public facing IP address c/w A record in DNS - one ORPS can support multiple WLCs
3. Put in place authentication filters to ensure that rubbish auth requests containing malformed/bad/nuisance usernames are not sent to the eduroam(UK) servers
4. Put in place RADIUS attribute filters to remove spurious/troublesome attributes that may ‘leak’ out of your own and other member organisation services as required in the eduroam(UK) Technical Specification
5. Comply with the eduroam(UK) Technical Specification RADIUS logging requirements [8]
6. Allow for upgrades/replacement of WLC separate from RADIUS service function

(*) There are several top quality RADIUS server systems available: FreeRADIUS, Aruba ClearPass, Microsoft NPS, Radiator, Cisco ISE etc

How do you configure a Cisco 1200 Series Wireless Access Point for eduroam SSID?

Details of the precise (largely web-based) steps used to configure the eduroam SSID on a Cisco® 1200 series WAP can be found in Appendix 2 of the case study Complying with the Janet eduroam Service Technical Specification.

Can Cisco fat WAPs be used with multiple broadcast SSIDs and dynamic VLANs?

There is a known problem with Cisco 'fat' WAPs with regard to multiple BSSIDs and dynamic VLAN assignment (RADIUS-assigned VLANs) which unfortunately affects a lot of institutions. The problem was that Cisco 'fat' IOS driven APs until recently only supported a single primary (guest) SSID broadcast in the beacons (the BSSID). Furthermore, it was not possible to achieve assignment of VLANs via RADIUS. This limitation does not apply to Cisco's 'thin' architecture, so the problem could hitherto only be circumvented by adopting this technology.

This issue only affected the autonomous Cisco APs. There never was any difficulty with lightweight APs (including upgraded autonomous ones) in supporting RADIUS-assigned VLANs and multiple broadcast SSIDs. (Certainly 1131 and 1232 APs in non-autonomous

LWAPP thin client mode with WiSM controllers have always worked fine).

With release 12.3.8-JEC(GD) of the Cisco IOS firmware, this issue has been resolved - certainly multiple BSSIDs with RADIUS assigned VLANs have been successfully setup with AP1231 and other 1200 series access points.

Although the issue has been resolved in the IOS, you may find that some AP radios do not support multiple BSSIDs. To find out if a particular radio will support multiple BSSIDs:

Run a 'show controllers' *radio_interface* command to check how many BSSIDs an AP will support. Look for the line which states - "Number of supported simultaneous BSSID on Dot11Radio0: 8", or something similar.

To set up multiple BSSIDs on the AP you can log into the web interface and select Security > SSID Manager. The page displayed will show the current VLANs configured and indicate which are being broadcast.

Alternatively from the IOS command line, enter SSID configuration interface and use the command mbssid. You'll also have to use mbssid from the configuration terminal interface to enable multiple basic SSIDs on an access point radio interface. This command was introduced in IOS release 12.3(4)JA.

See: Cisco IOS mbssid command [9]

[NB. The validity of following advice with regard to latest release of IOS is unknown - it certainly applied to pre-12.3.8 releases]. The Cisco WAP beacon can by default advertise only one broadcast SSID, nevertheless it is possible to alert client devices of additional SSIDs although this did not remove the limitation that RADIUS-assignment of VLAN was not possible. You can achieve client alerting of multiple SSIDs as follows; use the SSID list information elements (SSIDL IEs) in the access point beacon to alert client devices of additional SSIDs on the access point. When you designate an SSID to be included in an SSIDL IE, client devices detect that the SSID is available, and they also detect the security settings required to associate using that SSID.

See: Cisco AP Configuration Guide - Configuring Multiple SSIDs [10].

The AP configuration needs to use the command: information-element ssidl [advertisement] [wps](Microsoft Wireless Provisioning Services) [11] in the radio interface configuration / specific SSID configuration section.

For WinXP users the following download must be installed. This update enhances Windows XP support for Wi-Fi Protected Access 2 (WPA2) options in Wireless Group Policy (WGP), and helps prevent the Windows wireless client from advertising the wireless networks in its preferred networks list.

WinXP Update:

- http://www.microsoft.com/downloads/details.aspx?familyid=2726F32F-D52B-4F84-ACE8-F7FC20195769&displaylang=en [12]!!!
- http://support.microsoft.com/kb/917021 [13]

Using this update, the 'hidden' SSIDs become visible in a Cisco 'fat' AP environment - the

subsequent SSIDs use the extension made available through 802.11i.

Can you expand on what is necessary to convert 'fat' Cisco WAPs into 'thin' ones? (Is it just an IOS upgrade and does it cost anything? What device(s) do you use to control them? Do you lose any functionality in converting to thin?)

Changing to thin is a straightforward job. Either use the IOS command line (archive download-sw tftp://.....), the windows-based upgrade tool [14] or a WLSE (Wireless LAN Solution Engine). The upgrade tool and software image can be downloaded free from Cisco [14], and the tool pushes the image to the APs you tell it to, which converts them to lightweight. They then get their configuration from the controller rather than it being stored locally.

To control these thin APs you need a central controller, which incurs a cost. Lightweight wireless means all the clever stuff (authentication, key management, channel and power management) is done by a central box. This could be the Wireless Services Module (WiSM) for the Cisco Catalyst 6500 switch [15] (controls upto 300 APs), the standalone Wireless Control System (WCS) [16] or theCatalyst 3750G Integrated Wireless LAN Controller [17] (can only control about 32 APs). There's a fair amount of configuration to do so the controller knows about your VLANs, SSIDs, RADIUS servers etc.

You gain a great deal of functionality and management facilities - such as reporting, accounting, configuring WLANs, mobility etc. You manage the APs bia a web interface on either the controller or a PC running Cisco's WCS software, which co-ordinates multiple controllers and does RF planning etc. Adding a new access point is a straightfoward task of connecting it to a switch and then using the software to put the switch port in the right VLAN.

Summary:

- WAPs must have IOS 12.3(7)JA or higher
- Thin IOS must then be loaded via WinXP program (available on Cisco web) or via CLI
- The WAPs must be 1240AG/1130AG/1200 series [1210,1220,1230,1235]
- (1200 series radios must be one of following models only: MP21G/MP31G/RM21A/RM22A)
- Wireless controller module (WiSM) of some description necessary [WiSM for Catalyst 6500 (will need a free slot), WCS or Catalyst 3750G IWLC]
- Catalyst 6500 requirements: free slot for WiSM, Supervisor Engine 720 [18] WS-SUP720 needed and to run a SUP720 you need the higher rated PSU
- For large deployments of three or more WiSM, a WCS is recommended

There is a guide to the process on the Cisco web site: Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode [19]

To get the upgrade tool and Cisco IOS release:

- Browse to the wireless downloads page: http://www.cisco.com/en/US/products/hw/wireless/index.html [20]
- Click Access Points.
- Click the type of access point that you want to upgrade. When you click the access point type, the access point folder expands.
- Click the access point that you want to upgrade in the expanded list. The Select a Software Type list appears.

- For the upgrade tool, click the Autonomous to Lightweight Mode Upgrade Tool link.
- For the software image, click the Autonomous to Lightweight Mode Upgrade Image link.

Will a client configured for WPA2 fallback to WPA in a WPA-only environment?

Solving/mitigating the Overlapping eduroam Visitor service Problem (the 'Russell Square' Problem)

The overlapping eduroam service scenario is a well-known issue in eduroam. In the UK the way to address this is for organisations sharing the same locale to talk to each other and co-operate to minimise the overlapping Wi-Fi zones. This can be achieved by careful positioning of APs, reducing radio power and using non-omnidirectional antennae.

Other solutions require even closer co-operation and involve partial integration of networks (for instance the bigger organisation could provide Wi-Fi service across both campuses, providing an eduroam Visited service for both, and establish local RADIUS peering with the co-located organisation).

Can you expand on what is necessary to convert 'fat' Cisco WAPs into 'thin' ones? (Is it just an IOS upgrade and does it cost anything? What device(s) do you use to control them? Do you lose any functionality in converting to thin?)

Changing to thin is a straightforward job. Either use the IOS command line (archive download-sw tftp://.....), the windows-based upgrade tool [14] or a WLSE (Wireless LAN Solution Engine). The upgrade tool and software image can be downloaded free from Cisco [14], and the tool pushes the image to the APs you tell it to, which converts them to lightweight. They then get their configuration from the controller rather than it being stored locally.

To control these thin APs you need a central controller, which incurs a cost. Lightweight wireless means all the clever stuff (authentication, key management, channel and power management) is done by a central box. This could be the Wireless Services Module (WiSM) for the Cisco Catalyst 6500 switch [15] (controls upto 300 APs), the standalone Wireless Control System (WCS) [16] or theCatalyst 3750G Integrated Wireless LAN Controller [17] (can only control about 32 APs). There's a fair amount of configuration to do so the controller knows about your VLANs, SSIDs, RADIUS servers etc.

You gain a great deal of functionality and management facilities - such as reporting, accounting, configuring WLANs, mobility etc. You manage the APs bia a web interface on either the controller or a PC running Cisco's WCS software, which co-ordinates multiple controllers and does RF planning etc. Adding a new access point is a straightfoward task of connecting it to a switch and then using the software to put the switch port in the right VLAN.

Summary:

- WAPs must have IOS 12.3(7)JA or higher
- Thin IOS must then be loaded via WinXP program (available on Cisco web) or via CLI
- The WAPs must be 1240AG/1130AG/1200 series [1210,1220,1230,1235]
- (1200 series radios must be one of following models only: MP21G/MP31G/RM21A/RM22A)
- Wireless controller module (WiSM) of some description necessary [WiSM for Catalyst 6500 (will need a free slot), WCS or Catalyst 3750G IWLC]
- Catalyst 6500 requirements: free slot for WiSM, Supervisor Engine 720 [18] WS-SUP720

needed and to run a SUP720 you need the higher rated PSU
- For large deployments of three or more WiSM, a WCS is recommended

There is a guide to the process on the Cisco web site: Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode [19]

To get the upgrade tool and Cisco IOS release:

- Browse to the wireless downloads page: http://www.cisco.com/en/US/products/hw/wireless/index.html [20]
- Click Access Points.
- Click the type of access point that you want to upgrade. When you click the access point type, the access point folder expands.
- Click the access point that you want to upgrade in the expanded list. The Select a Software Type list appears.
- For the upgrade tool, click the Autonomous to Lightweight Mode Upgrade Tool link.
- For the software image, click the Autonomous to Lightweight Mode Upgrade Image link.

Will a client configured for WPA2 fallback to WPA in a WPA-only environment?

Solving/mitigating the Overlapping eduroam Visitor service Problem (the 'Russell Square' Problem)

The overlapping eduroam service scenario is a well-known issue in eduroam. In the UK the way to address this is for organisations sharing the same locale to talk to each other and co-operate to minimise the overlapping Wi-Fi zones. This can be achieved by careful positioning of APs, reducing radio power and using non-omnidirectional antennae.

Other solutions require even closer co-operation and involve partial integration of networks (for instance the bigger organisation could provide Wi-Fi service across both campuses, providing an eduroam Visited service for both, and establish local RADIUS peering with the co-located organisation).

Archive Questions:

Will an AP configured for WPA2 fallback to WPA if a WPA-only client tries to associate?

The native Windows XP supplicant software requires the user to make an explicit choice between WPA and WPA2 when performing the configuration. If a user with a device configured for WPA2 visits a site where the guest WLAN has been configured to utilise WPA, will they be denied service, or does the client fall back to WPA? Similarly if the guest WLAN has been configured for WPA2 and a visitor arrives with a device configured for WPA will the APs fall back to support WAP or will the user experience problems?

It will probably be the case that a client set up to use WPA2 will not work at a WPA location - this depends on the supplicant and the configuration. Generally a client needs to have the correct specific cipher methods configured. Likewise a client configured to use WPA will not work in a WPA2-only location.

Some clients can handle both WPA and WPA2 versions of the same SSID... and some clients (eg Vista) can even have different profiles pointing to the same SSID. See Workstation/Laptop Setup [21] above.

However, since the vast majority of clients only support WPA at present, we advise that JRS3 WPA2 sites should still provide WPA connectivity and JRS2 sites must provide WPA (and they may also provide WPA2). This advice will stand until we see a wholesale migration to WPA2 (which is expected in a few years time).

Our Cisco 1200 autonomous-mode APs have been configured using the 'cipher' option of 'AES CCMP + TKIP'. Does this mean that our WLAN is effectively supporting both?

Yes, it should support both - you can determine this by using a wireless card or probe that tells you what ciphers it can detect, eg. the 'airport' utility in MacOSX.

We recommend that the cipher mix is kept to the standards - eg WPA/TKIP and WPA2/AES.- Whilst WPA/AES exists it is very exotic and WPA2/TKIP is just wrong.

Another reason to implement WPA2/AES (alongside WPA/TKIP) is that only with AES can true 802.11n speeds be obtained (apart from in a wide open wi-fi scenario) - so anyone looking at 802.11n kit needs to keep this in mind.

Useful links:

- Wireless assistance\\Tech Guide: Wi-Fi: Security For The Masses [22]
- 802.1X Port Access Control for WLANs [23]
- Deploying 802.1X for WLANs: EAP Types [24]
- Wireless on Linux, Part 1 [25] and Part 2 [26]
- Open1X.org - Selecting An Appropriate EAP Method For Your Wireless LAN Evolution of WLAN Security [27]

11) Supporting Users

What sort of support for users to we need to provide?

We would expect organisations providing eduroam services to provide their users with adequate support; as a minimum, in addition to the organisation's eduroam service information web pages which must provide help on how to use eduroam and device set up instructions, the organisation's IT helpdesk should have the capability to:

- provide guidance on the set up of users' devices for operation with eduroam
- check the status of a user's account to ensure that they are eligible to use eduroam
- check RADIUS logs to see if authentication requests are being received for the user's authenitcation attempts and the outcome of those attempts

PS We have published a supporting users troubleshooting flowchart, designed for help desks which may be of some help:
eduroam-users-troubleshooting-flowchart-it-support-staff.pdf [28]

How do I get access to the eduroam CAT (Configuration Assistance Tool) web site?

To use the eduroam CAT tool (developed through the Geant eduroam confederation), you

need to have a compliant Home service and an invite token. To get a invite token go to your eduroam(UK) Support server main configuration page and click on the eduroam CAT invite button. A token will be sent **to the e-mail address you have registered as the primary technical contact** on the web site. **The token expires after 24 hours**, so must be used before then. (Nb. If you have only just changed your compliance assertion on eduroam(UK) Support server you will have to wait until the update replicates through to the European database for your organisation to be listed on CAT).

For more information see eduroam CAT [29].

What do I need to do to get my federated access SSO service to support my sys admin access to CAT?

Your federated access SSO IdP needs to release eduPersonPrincipalName and eduPersonTargetedID attributes to the https://monitor.eduroam.org/sp/module.php/saml/sp/metadata.php/default-sp [30] SP. It may be the case that your IdP will release these without any further configuration or you may find that your IdP needs to be modified.

Create policy for cat.eduroam.org attribute release

The **attribute-filter.xml** file needs to have this policy in place before your sign on will function

```
<afp:AttributeFilterPolicy>
<afp:PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="
<afp:AttributeRule attributeID="eduPersonPrincipalName">
<afp:PermitValueRule xsi:type="basic:ANY" />
</afp:AttributeRule>
<afp:AttributeRule attributeID="eduPersonTargetedID">
<afp:PermitValueRule xsi:type="basic:ANY" />
</afp:AttributeRule>
<afp:AttributeRule attributeID="cn">
<afp:PermitValueRule xsi:type="basic:ANY" />
</afp:AttributeRule>
<afp:AttributeRule attributeID="mail">
<afp:PermitValueRule xsi:type="basic:ANY" />
</afp:AttributeRule></afp:AttributeFilterPolicy>
```

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 [31]

What is the 'eduroam(R) via partner' profile that is installed alongside the 'eduroam(R)' profile?

Prior to CAT release 2.1.2, When using the 'classic' CAT installer, when you run the executable (Windows), the 'Welcome to the eduroam(R) installer' screen advises that wireless profiles will be created: 'eduroam(R)', eduroam(R) via partner' and if additional Hotspot 2.0 Consortiums are set up by the CAT administrator, 'Organisation Custom Network'.

From CAT 2.1.2 onwards the designation eduroam(R) has been removed - to avoid the confusion that was caused by the SSID supported always being 'eduroam'.

Profiles installed via the CAT installer:
The 'via partner' profile is a Hotspot 2.0 profile ('settlement free' RCOI)
'Organisation Custom Network' will be installed if you as CAT Administrator add configuration to the EAP profile via the 'Media properties for this profile' box by ticking the 'Additional HS20 Consortium OI' or 'OpenRoaming' options.

7) 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 [32]

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 [33] (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 addess, password etc.

Links
[1] https://www.jisc.ac.uk/events/wireless-mobility-event-27-feb-2019
[2] http://www.revolutionwifi.net/revolutionwifi/p/ssid-overhead-calculator.html

[3] https://wiki.geant.org/pages/viewpage.action?pageId=131634132
[4] http://optimise-your-wlans-for-phones-and-tablets
[5] https://www.jisc.ac.uk/frameworks
[6] https://www.jisc.ac.uk/network-equipment-framework
[7] https://community.jisc.ac.uk/system/files/56564/Network%20Equipment%20-%20Buyers%20Guide%20v.6.pdf
[8] https://community.jisc.ac.uk/library/janet-services-documentation/clarification-eduroamuk-policy-and-tech-spec-wording-visitor
[9] http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/command/reference/cr12410b-chap2.html#wp2700587
[10] http://www.cisco.com/en/US/docs/wireless/access_point/12.3_7_JA/configuration/guide/s37ssid.html#wpxref78332
[11] http://www.microsoft.com/technet/community/columns/cableguy/cg1203.mspx
[12] http://www.microsoft.com/downloads/details.aspx?familyid=2726F32F-D52B-4F84-ACE8-F7FC20195769&displaylang=en
[13] http://support.microsoft.com/kb/917021
[14] http://www.ja.net/services/authentication-and-authorisation/janet-roaming/technology.html#cisco_AP_thin_upgrade_tool
[15] http://www.cisco.com/en/US/products/ps6526/index.html
[16] http://www.cisco.com/en/US/products/ps6305/index.html
[17] http://www.cisco.com/en/US/products/ps6915/index.html
[18] http://www.cisco.com/en/US/products/hw/modules/ps2797/ps5138/index.html
[19] http://www.cisco.com/en/US/products/hw/wireless/ps430/
[20] http://www.cisco.com/en/US/products/hw/wireless/index.html
[21] http://www.ja.net/services/authentication-and-authorisation/janet-roaming/technology.html#multiple_encryption_profile_Vista
[22] http://www.informationweek.com/story/showArticle.jhtml?articleID=10808186
[23] http://www.wi-fiplanet.com/tutorials/article.php/3073201
[24] http://www.wi-fiplanet.com/tutorials/article.php/3075481
[25] http://www.wi-fiplanet.com/tutorials/article.php/3066371
[26] http://www.wi-fiplanet.com/tutorials/article.php/3081601
[27] http://open1x.sourceforge.net/links.html
[28] https://jisc365.sharepoint.com/:b:/s/PublicDocumentLinks/EZDTqQ6rTGVFn0p_xquaAJQBAjUKSPXggAll5lqj5JjTHA
[29] https://cat.eduroam.org/
[30] https://monitor.eduroam.org/sp/module.php/saml/sp/metadata.php/default-sp
[31] https://social.technet.microsoft.com/Forums/windowsserver/en-US/e73183d4-7b2f-48a7-9246-97ed711e8e8d/eappeapmschapv2-realm-stripping?forum=winserverNAP
[32] http://www.novell.com/documentation/edir_radius/index.html
[33] http://wiki.freeradius.org/FreeRADIUS_Active_Directory_Integration_HOWTO