Implementing Govroam Roadmap

Concepts and Terminology

It is recommended that organisations planning to implement Govroam familiarise themselves with the concepts and terminology described in the

High Level Architecture

document.

Notes and Caveats

This document is based on modified eduroam implementation guide.

Aspects of this document are out of date and are due for updating.

Many of the external documents referred to are eduroam specific. While they should still be applicable to Govroam there may be some small differences. There will be Govroam specific versions made available over time and this document updated accordingly.

Resources:

There are useful summaries of concepts and infrastructure components in the European Govroam wiki, which may of help if there any questions unanswered from this web page: general_overview

Govroam version required: https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-Generaloverview

and elements_of_the_govroam_infrastructure

Govroam version required: https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-Elementsoftheeduroaminfrastructure

.

Recommended reading: for an introduction to 802.1X, chapters 1 and 2 of 802.1X Implementation at Janet-Connected Organisations

 Updated or Govroam specific version required.

Jisc factsheet: IEEE 802.1X

 Updated or Govroam specific version required.

Jisc factsheet: EAP Extensible Authentication Protocol

 Updated or Govroam specific version required.

Deciding your service type and planning your Govroam implementation

In the UK, organisations generally fund and deploy their network systems independently with the result that there is a wide range of ways in which organisations have implemented network services. To enable disparate networks to interoperate for the purpose of user authentication and to provide a reliable and predicable service for the user, Jisc has produced the

Govroam Technical Specification

. This defines the service types and the technical standards that must be adhered to by all participating organisations.

Decide the type(s) of service you wish to provide

The first step in planning your Govroam implementation is to decide the type(s) of service you wish to offer for visitors and for your own users and that will best suit your organisation. There are several factors which may influence your decision. Most participants choose to deploy both a Home and a Visited service and Jisc encourages this approach. Choose from:

a) Visited only organisation: you provide an Govroam connectivity service for visitors to your locations. This may be appropriate if you have no eligible users or are providing the service at a venue which only caters for visitors or you are providing a managed service for a client institution.

b) Home only organisation: your members will be able to benefit from Govroam at other sites. Building a Home service is perhaps technically the most challenging component since the RADIUS server must process authentication requests, acting as an EAP end point and performing user database lookups to your AD/LDAP etc.

c) Home and Visited: you enable Govroam connectivity for your Govroam-enabled network users for when they roam to other sites and you reciprocate by providing an Govroam connectivity service to support visitors to your site. Your Govroam service can also provide Govroam connectivity for your

own users (although you are not under any obligation to provide such connectivity for your own users). If you do authenticate your own users via Govroam on your own site, you may connect them to your Govroam visitors network, but you are not under any obligation to connect them to that. You can connect them to any of your other (non-Govroam) network services - which may be more appropriate since they are at their home site. The means to do this are described later in this guide.

Whilst you need a good idea of the aim of your Govroam deployment programme and be able to allocate sufficient resources in terms of server hardware, software and time, you don't need to decide every detail of the implementation of your service at the start of the process. Building of a comprehensive Govroam service can be tackled in stages. Indeed a step by step approach is recommended - the various areas are described in this 'roadmap' guide. Technical Support can provide advice and guidance for your project at each stage of implementation.

Recommended viewing - video of James Hooper's presentation overview of the Govroam deployment at Bristol, 'Challenges for wide scale 802.1X deployment'

Eduroam specific. Can we do a Govroam version? Mark?

. For slideset, see 'Resources' at bottom of this section. Although showing it's age now, this is a comprehensive overview of Govroam deployment and can be viewed in parallel with the notes below. Govroam CAT is not covered and references to 'Janet' and 'JRS' should now be understood as 'Jisc' and 'Govroam'.

Consider Wi-Fi and Network Architecture if offering Visited Service

All Govroam services require you to deploy a RADIUS service. Ideally this should be a resilient service and comprise two servers, which may be physical boxes or virtual machines. Selection of the RADIUS server software is covered in the following section.

Consider the technological aspects of the network you wish to offer Govroam over. To provide a reasonably standard experience for users and to try reduce the amount of changes to supplicant and application settings required from site to site, the Tech Spec currently defines a single sets of network parameters based on WPA2 'enterprise' authentication with AES encryption.

Post-authentication walled-gardens such as where users must click e.g. 'Accept' or load a virus scanner before being admitted to the network are however still permitted. Such systems may be employed for example to assure acceptance of conditions of use or to ensure device patching is up to date or other SoH standards.

Although not recommended?

Decide EAP methods to support for Home services

If you decide to offer a Home service, you need to decide what EAP authentication mechanism(s) you want to employ. This is an important decision since it will affect how your user's devices must be configured and the driver/supplicant software and certificates needed. The supplicant requirements

may also affect how you support installation/configuration, whether an automated client config system can be used and the provision of instructions for your users. The decision on EAP mechanism will also probably involve a review your WLAN setup - if your site has one (nb. you don't need to have a WLAN on your home network site in order to provide an authentication service for your users when they are visiting other organisations and using the remote site guest WLANs).

Your choice of EAP mechanism will be determined by:

1. the RADIUS platform you choose(e.g. Microsoft NPS only supports PEAP/MSCHAPv2 and EAP-TLS)
2. how the credentials on your authentication backend are held/encrypted,
3. the authentication backend system (AD/LDAP)
4. the rate of authentications and the number of simlutanteous authenticated users your system will support (some software engines may lack sufficient performance)
5. the device operating systems you wish to support and
6. the supplicant software you have or plan to install/use on the client devices and may also be influenced by your wireless LAN (if any) setup/vendor support. This may sound complicated, but for smaller organisations the range of options is limited and the decisions are quite easy to make. Seek advice from our tech support team if in doubt.

Consider how users devices are to be configured to work with the service

The method of deploying configuration of the supplicants on devices should be given some thought. Whilst it is possible to just let users do this themselves, this approach will inevitably lead to calls to your helpdesk, user frustration and importantly, insecure device configuration due to incomplete setup of authentication server certificate and server name validation. It is a requirement that you provide device setup instructions but some form of automated setup tool/help system for users is strongly recommended. The section below on User Device Setup gives more details. A number of organisations have implemented open access captive portal setup networks which provide access to their automated setup tools for first time users.

Further Considerations

For participants deciding to offer Visited services (ie most organisations!), a further set of issues must be addressed, particularly the implementation of Govroam VLAN assignment on your wireless access points and wired switches. Also your firewall from the Govroam network/VLAN must permit certain traffic types as detailed in the Firewall Configuration section below.

Without wishing to complicate the process more than necessary, you may wish to consider whether or not you wish to provide guest network services to non-Govroam visitors. These may be visitors from UK organisation not participating in Govroam, overseas visitors, delegates from outside the community to conferences and contractors. Some organsations only offer Govroam services now!

True?

Recommended reading is the Jisc guide on provision_of_network_access_for_guests

Govroam version required: https://community.jisc.ac.uk/library/janet-policies/guest-and-public-network-access

- the simplest method is through a 'Guests' SSID with a separate non-Jisc network feed. You may at the present time however provide guest accounts for use with your Govroam service, but only on strict conditions.

Is discussion of visitor access applicable to Govroam? No eVA equivalent. Govroam **is** the guest access.

Help is available on all aspects of planning your service from Govroam Technical Support

Resources:

- Challenges for wide scale 802.1X deployment video < highly recommended viewing

Eduroam specific

- Challenges for wide scale 802.1X deployment slideset < high quality slideset

Eduroam specific

- deployment_guide

Govroam version required https://community.ja.net/library/janet-services-documentation/eduroam-deployment-guide

- Technical Specification
- Comparison of supplicants
- inter-nren_roaming_infrastructure_service_support_cookbook

Missing. Found a copy and it's eduroam specific and '07 vintage.

(pdf) (produced and published by GEANT2)

- Consult Technical Support for advice

Choose RADIUS server platform and plan network connectivity for ORPS

Choice of Platform

The RADIUS server platform selected will be influenced by the type of credentials employed at your organisation (AD, NDS, LDAP and how certificates are utilised) and consequently the EAP types that you could use. This in turn will affect the choice of supplicant and that may also affect the decision. Other factors will be vendor preference, budget and technical expertise. Most RADIUS platforms however support a wide range of EAP types and authentication back-ends.

Options:

- FreeRADIUS website
- Radiator website
- Microsoft Network Policy Server (NPS) (Windows Server 2008)
- Cisco ISE
- Aruba Clearpass
- Juniper Funk Steel-Belted Radius website
- Radsecproxy

Your ORPS may be physical machines or may be VM-based

Network Architecture

There is no best practice recommendation regarding positioning of your ORPS function in your network architecture. You can connect your ORPS into a DMZ or you can connect it to your internal network to facilitate access to your LDAP/AD. The decision as to where to connect it is up to the organisation and will probably be based on existing security policy.

Whatever you choose, the firewall requirements are described later in this guide. Note that in the current UDP*/RADIUS-hierarchical model for Govroam, only the NRPS will communicate with your ORPS so security can be very tight. Unlike, for instance web servers, which need to be open to the wide Internet, your ORPS operates only in a very narrow RADIUS environment. ([*] Technically you could employ RadSec TLS/TCP, (applicable only to Radiator and FreeRADIUS 3), but again the only communications will be with the NRPS, at present) - Nb. this is not an implementation we are currently advocating).

Your ORPSs must have IP addresses that are reachable and that are resolvable by DNS lookup from the NRPS so if you do wish to employ network address translation, this must be fixed.

Note - 'cloud' based ORPS solutions have not been tested and evaluated by Govroam. Provided that any such solution can meet the Technical Specification they are not prohibited, but Govroam cannot endorse their use.

Separation of RADIUS duties

It is worth considering that the RADIUS proxy server you define as your ORPS does not necessarily need to do any authentication itself. It is perfectly OK to use a relatively simple proxy-only RADIUS server facing Govroam which then forwards any authentication requests received to your NPS server or as needed. One scenario where you might chose to do this is where your chosen RADIUS platform cannot do Operator-Name injection or respond to Status-Server requests or which has poor attribute filtering capabilities and you want to implement these best practice techniques. Another scenario might be that you wish to dedicate an internal RADIUS server to authentication duties and separate the 'proxying' to a second server. FreeRADIUS or radsecproxy make an ideal platform for the proxy-only server in these models.

Resilience

Once your users have experienced Govroam, they will very rapidly come to regard it as an indispensible feature of your network service and your ORPS will become a very important component. Furthermore, once your ORPS have linked into the RADIUS hierarchy of Govroam the NRPS will normally expect your organisation to be responsive to RADIUS requests sent to your realm. Whilst there is now logic in place to cope with non-responsive ORPS, it is good neighbourly practice to ensure that your ORPS are up and operational 24/7. It is therefore strongly recommened that participants deploy at least two fault tolerant servers for resilience. The NRPS will communicate with these in the order in which they were configured, but you will be able to adjust the priority.

Your two ORPS will normally be configured with separate unique shared secrets for communication with the NRPS, but you can opt for the same shared secret to be used on both servers (make you request through Jisc Service in the normal way). organisations with Cisco ISE or Aruba Clearpass solutions will probably require this.

Help:

Consult Technical Support for advice

FAQs:

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 sofware, including the following:

FreeRADIUS – Version 3 is the current major release. Known vulnerabilities.

Radiator - Known vulnerabilities

Select your Realms and Join Govroam

Selecting your realm

An important parameter to decide is your organisational realm name. This will form the second part of your users' usernames and is effectively the organisation identifier used by Govroam RADIUS servers (at other member organisations and by the national and international Govroam infrastructure) to ensure that authentication requests can be passed back to your organisation when your users roam. The realm name is the '@holby.nhs.uk' part of the username (userID@realm).

Your organisation must be entitled to use the requested realm name, ie it must be (or be derived from) a DNS name from the organisation's registered DNS namespace. It is expected that most organisations will request their DNS domain name (eg. 'holby.nhs.uk') although it is perfectly acceptable to request a sub-domain name (eg. 'resus.holby.nhs.uk'). You cannot use internal AD container names (obviously these won't be configured in remote RADIUS servers nor will they be capable of NAPTR record lookups in DNS).

Nb. Your RADIUS server and authentiation platform will need to be able to handle the realm identifier in auth requests. Hint, in Microsoft AD this is usually achieved by using a suitable global UPNs (user principal name) in the AD. This is dcomented in Microsoft Active Directory and NPS technical manuals.

Complete the application form

The next step is to apply to joining the Govroam federation. This is a very straightforward process - you simply complete the membership application form, which asks for contact and intended Govroam service deployment details. The online form must be endorsed by a senior member of your organisation.

Complete and submit the Govroam application form. Following a validation check and acceptance of your membership to the Govroam federation a welcome information pack will be e-mailed sent to you. Once the financials have been arranged and Terms and Conditions signed then we can use the information provided to on-board your RADIUS servers. The relevant information about the Jisc RADIUS servers will be sent to a nominated technical representative.

FAQs:

What support services are available?

To underpin the service and to support organisations joining and participating in the service, a comprehensive, fully resourced support structure has been put in place which provides:

- Pre-deployment support – planning and selection of RADIUS server hardware and software and supplicant systems
- Technical support during implementation

- Post-implementation support on technical issues
- Test account for testing outgoing authentication (visitors).
- Website through for testing authentication of local account (home).
- Participanting organisations RADIUS service monitoring system

Would be nice.

- Dedicated e-mailing list for technical and service announcements
- A chargeable consultancy service
- Comprehensive technical and promotional documentation
- Locations map showing where Govroam is available and the service details at each site
- Client onboarding tool, the Configuration Assistant Tool (CAT).

Can individuals join Govroam from Jisc? Is there a way for an individual to obtain an Govroam ID without the user's home institution having to join Govroam?

No. Users must have registered network logon accounts at their home organisations and in order for individuals to use their credentials for authentication at Govroam participating sites, their home organisation has to join Govroam and install a RADIUS server which is peered with the Govroam infrastructure.

The aim of Govroam is to reduce the amount of administration required both by organisations offering guest access to their networks and for visiting users. This is achieved by users being enabled to use their own usernames and passwords when roaming. Jisc has set up the NRPS network and the support service to facilitate this through the Govroam mechanism. There is no facility for users to be issued with independent IDs since this would involve another tier of administration (and defeat the aim of the service).

Do Govroam users have to be registered network logon account users at participating organisations?

Yes. Users must have a network account at their participating home organisation in order for their authentication requests to be validated when they attempt to log on at a visited organisation. They must be registered on their home organisation's AD, LDAP, NetWare etc user database. This is because Jisc connected organisations are not permitted to just let anyone onto their guest networks and to access Jisc/the Internet via Jisc. Furthermore, there is a logging requirement for organisations to record the date and time and user name of Govroam enabled authentications. We have to be able to track down a visiting user if ever there is any security or anti-social usage incident - hence the need to limit the service to registered users.

Can I have a sub-realm for my organisation?

Question a) Does the Govroam spec allow us to configure ORPS to forward user@department.myorganisation.ac.uk RADIUS requests to the department in question's

RADIUS server?

Answer a) Yes - you can submit any number of sub-realms (such as 'department.myorganisation.ac.uk' as you like by sending an email request to govroam@jisc.ac.uk.

Question b) If so, will the NRPS strip off 'department' and forward RADIUS requests to the example-org ORPS?

Answer b) No - the NRPS will forward requests bearing these realms to your ORPS unchanged. Because the realm is left unchanged by the NRPS, you can perform additional proxying within your organisation if you wish (for example, to route the request to a departmental RADIUS server). This permits delegation of authentication to other units within your organisation.

Can I request a wild-card realm?

No - however, you are able to define as many “sub-realms” as you require. For example, if your realm is example.ac.uk, you can additionally define bar.example.ac.uk and foo.bar.example.ac.uk.

Support Server Section

Install Your RADIUS Server (ORPS)

If you have not already implemented RADIUS on your network, a RADIUS server of your choice must now be deployed. We recommend that software is installed on dedicated hardware or on a virtual platform. Your ORPS must have a unique public-facing IP address and FQDN. The first step is therefore to give your server a DNS name and to create an entry in your DNS zonefile. Next you carry out basic installation of your selected software.

It is strongly recommended that your ORPS is highly fault tolerant and preferrably a resilient dual-ORPS system is put in place. This will require configuration of fail-over or load balancing between the two ORPS. Different systems have differing requirements, but normal practice is for each of your ORPS to have a unique set of shared secrets with the NRPS (the shared secret between roaming0 and ORPS1 will be different from the secret between roaming0 and ORPS2). If your configuration requires both ORPS to have the same shared secret for each NRPS, please open a service request ticket with Govroam Service Desk and we will configure the NRPS accordingly. Acquiring shared secrets for ORPS. Nb. Each of your ORPS must have a unique IP address and FQDN, if you are using NAT for some reason you'll need to have static translation in place.

The reason we strongly recommend you depoly a resilient dual-ORPS system is two-fold, a) for your own service continuity b) but most importantly from an Govroam viewpoint, to ensure that your realm always has an ORPS available to service incoming authentication requests from the NRPS. If your realm for some reason stops responding to auth-requests and these continue to arrive from your users at remote Govroam sites, a huge amount of NRPS resources will rapidly become tied up and the performance of the NRPS will be drastically reduced. This is because since RADIUS uses UDP, each auth-request results in a UDP socket being held open in the NRPS UDP buffer awaiting a reply. If your

realm continues to fail to reply, the load on NRPS resources will increase to the point that effectively service will be denied to other operational Govroam sites - which are handling auth-requests properly. To prevent this situation from affecting the performance of the national service, Govroam will have no option but to suspend service to your ORPS.

Resources:

inter-nren_roaming_infrastructure_service_support_cookbook


Missing

- covers various RADIUS platforms (dates from 2008, but still very useful) - 404 error now

1. FreeRADIUS
    - FreeRADIUS official website
    - Janet 802.1X Implementation at Janet-Connected Organisations - an introduction to FreeRADIUS installation and configuration
    - FreeRADIUS Demystified Seminar - Alan Buxey's seminal 2012 pre-NWS40 FreeRADIUS Demystified seminar presentation


Out of date and/or eduroam specific

- FreeRADIUS Best Current Practice Configuration for Govroam - partner material for the FR Demystified seminar


Out of date and/or eduroam specific

- FreeRADIUS Packet handling; examining the flow - partner material for the FR Demystified seminar


Out of date and/or eduroam specific

- Govroam.org wiki - FreeRADIUS setup


Out of date and/or eduroam specific

1. Radiator
    - Radiator official website
    - Govroam.org wiki - Radiator setup


Out of date and/or eduroam specific

1. Microsoft NPS
    - Microsoft NPS Configuration Guide - produced by Govroam, step-by-step NPS RADIUS setup guide with screenshots

Out of date and/or eduroam specific

- Using Windows NPS as RADIUS in

Out of date and/or eduroam specific

- edu

Out of date and/or eduroam specific

- roam - produced by UUINETT (Norway) so beware of country-specific content, but includes content covering AP config and certificates

Out of date and/or eduroam specific

- Microsoft NPS website documentation

Out of date and/or eduroam specific

- Deployment of IEEE 802.1X for Wired Networks Using Microsoft Windows
- Deploying MS NPS with VLANs

Out of date and/or eduroam specific

1. Aruba ClearPass
    - Guide to Configuring Aruba WLC and ClearPass - written by UUINETT and likely to have Norway-specific config content!

Out of date and/or eduroam specific

1. Cisco ACS / ISE
    - cisco_ise_configurationSee material in the Library


Eduroam specific. Govroam version needed?

Acquire Server Certificate for ORPS/NAS

Depending upon the EAP method you choose to implement, mutual authentication between client and RADIUS server is generally required. The first stage of this is that the client machines need to be able to trust the authenticity of the RADIUS servers and network access servers/APs that they communicate with during the authentication process. The most popular EAP methods require that the authenticating RADIUS server must have a digital certificate. This can be from a legitimate certification authority (CA) or can be self-signed. Nb The recently defined EAP-PWD method does not require the RADIUS server to have a certificate, however it is not widely supported by suppliants.

Govroam services, being built on 802.1X, are generally implemented using EAP methods that use transport layer security (TLS), such as EAP-TLS, EAP-PEAP and EAP-TTLS - which require the use of a server certificate to authenticate the RADIUS server to the supplicants. In addition EAP-TLS also requires client certificates in order for the clients to be validated by the RADIUS servers. These client certificates may be self-signed, ie. generated by your private CA software.

Best practice is to utilise self-signed certificates. This eliminates the threat posed by the possibility of a malign agent setting up a RADIUS server masquerading as your ORPS and using a server certificate acquired from the same CA as your legitimate ORPS. Inadequately set up supplicants, those where server certificate name validation is not enabled, will be at risk of trusting the spoofed ORPS and so vulnerable to harvesting of credentials. Use of self-signed certificates will of course require these to be distributed to user's devices. It is recognised that many organisations will lack the time or resources to produce self-signed certificates and to manage the distribution of these to client devices, but this is our best practice recommendation. Jisc provide a way of generating self-signed certificates for testing purposes. They're specifically designed to be a compatible with Govroam (and eduroam) as possible.

If you decide not to use self-signed certificates, most RADIUS servers will work without difficulty using certificates from both root certification authorities and intermediate certification authorities . If you implement MS Internet Authentication Server however, particular care will be needed in configuring the server because by default it is assumed that the certificate is issued directly from a root certification authority known by the supplicant. This may also apply to NPS.

If you deploy multiple ORPS servers, since there is no technical requirement for each server to have a different certificate, it is recommended you use one certificate for all your ORPSs, thereby avoiding issues of support and client configuration/certification. The certificate will of course need to contain all the server names of the ORPSs you will be deploying it on and care will be needed when preparing the CSR.

Resources:

- EAP Server Certificate Considerations - highly recommended (almost mandatory) reading from the Govroam Europe documentation wiki
- Understanding Server Certificate Validation - video stream of Kevin Koster's presentation to

NWS

Eduroam specific.

- Factsheet: Introduction to Server Certificates
- Microsoft technical article: Certificate Requirements when using EAP-TLS or PEAP with EAP-TLS
- TechRepublic paper - Self-sign a RADIUS server for secure PEAP or EAP-TTLS authentication

Missing

- Advisory: Supporting Windows Mobile 8 Certificate Validation
- Advisory: MD5 certificate types deprecated in favour of SHA-1 for RADIUS server

FAQs:

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

Yes. EAP methods that use TLS, such as EAP-PEAP and EAP-TTLS, require the use of a server certificate to authenticate the RADIUS server to the supplicans.

This certificate may be derived from a local self-signed certificate authority (CA), or purchased from a commercial CA. The advantages and drawbacks of both of these are listed below.

Benefits of a certificate from a self-signed CA:

- No need to purchase a certificate from a commercial vendor.
- 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).

Benefits of a certificate from a commercial CA:

- No need to distribute the CA's root certificate to each client.

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

Add your ORPS to the Govroam RADIUS Infrastructure and Add NRPS to your ORPS

RADIUS config

You now need to peer your ORPS(s) with the NRPSs so that they can exchange RADIUS communications. This requires the addition of your RADIUS servers as clients in the relevant RADIUS server configurations together with the shared secrets that will establish trust. As stated in Install Your RADIUS Server, your ORPS needs to have a public facing IP address and a fully qualified domain name (an address record in DNS). Your ORPS will be configured in the NRPS clients tables with their IP addresses, but you need to provide us with the FQDNs. This reduces scope for error, facilitates IPv4 and v6 support and enables you to change the IP address in the future without needing to update Support.

Since a there are two ends of the RADIUS conversations there are two operations:

1. Addition of your ORPS to the RADIUS clients configuration of the NRPSs
2. Addition of the NRPS to the RADIUS clients configuration of your ORPSs

Add your first ORPS and Acquire your Shared Secrets

Follow the instructions most appropriate to your organisation:

- Public sector organisation joining as a full member
- Public sector organisation joining as a Visited Only
- University or third-party joining as Visited Only

The basic process is the same: fill in a form, or forms, send it/them to govroam@jisc.ac.uk and we'll send you the shared secrets and a test account for testing on-campus visitors.

Add the NRPSs as RADIUS clients on your ORPS

You will be emailed, securely, the shared secrets between the NRPS and your ORPs. These must be entered into the relevant RADIUS clients configuration files/fields on your ORPS servers. Accuracy is essential when transcribing shared secrets. Ensure that there are no extra characters (white space at beginning or end of the shared secret) and ensure that you are copying and pasting with a correct UTF-8 or ASCII buffer so that characters do not get adjusted when pasting from web browser.

The NRPS will be able to accept and send RADIUS packets from/to your ORPS(s) immediately.

There are four NRPSs and any one may try to communicate with your ORPS systems, so you must allow all NRPS to talk to your ORPSs (hint: FreeRADIUS, edit clients and proxy.conf files). You must configure your ORPS for roaming0.govroam.uk, roaming1.govroam.uk, roaming2.govroam.uk and roaming3.govroam.uk to have full auth passes - 1812 on UDP and be allowed as clients on your ORPS. It is essential that the NRPS are added to you systems using IP addresses and not the Roaming0/1/2/3 FQDNs! (The NRPSs are IPv6 capable and the addresses are resolvable through DNS. Windows 2012R2 and above NPS users note, NPS is IPv6 aware so if FQDNs are used the ORPS will do a DNS lookup and may select the v6 address and if your site is not fully IPv6 enabled, the ORPS will attempt

to tunnel v6 via v4 resulting in communications failure with the NRPS).

Setting up RADIUS forwarding/proxying.

Adding a Second/any Further ORPS

Additional ORPS can be added to the clients config of the NRPS by following the same steps as described above. It is now quite common practice for organisations to deploy multiple ORPSs, which they may do for resilience or load sharing. You can add as many ORPS as you wish.

Once an ORPS has been added the NRPSs will automatically communicate with it. NRPS send all traffic to the first ORPS in their config list until it stops responding, the NRPS then try the next ORPS in the list. The order of preference is the order which the ORPS were added to the Support server. If you want any particular ORPS to be your primary server, set the 'High priority' option on its config on the Support server, as indicated in section 9.1.

Shared secrets for your additional ORPS: Normally every ORPS has a unique set of shared secrets for peering with the NRPS. This is best practice and the most secure way of employing shared secrets. This remains true even in scenarios in which peered realms contain multiple RADIUS servers. When an organisation registers a second ORPS, by default a further unique set of shared secrets is generated, different from those for the first ORPS. Govroam administrators must be aware that in deployments where the ORPS form fail-over clusters you cannot simply use the original four shared secrets on both ORPSs.

We recognise however that there are particular solutions which use and require a common shared database for all clients and so require the same shared secret for each NRPS to be used by all ORPSs. Where two ORPS are deployed in fail-over systems that use the same set of secrets for each ORPS-NRPS proxy/client config. (ie ‘secret0’ for roaming0 for both ORPSs, ‘secret1’ for roaming1 for both ORPSs, etc.) we can, on request, adjust the details (ie we will duplicate the settings for one of your ORPS). This has had to be done for a number of sites that have chosen a cluster solution that doesn’t allow different keys for remote agents.

If this is required, please choose the ORPS that will be the nominal shared secret seed and which ORPS you want to have adjusted to be the same as that seed and let us know.

Firewall Configuration to Permit RADIUS Servers to Work with NRPS

The next step is to enable your RADIUS service to communicate with the national RADIUS Porxy servers. RADIUS uses UDP and so there is a requirement for the ports specified below to be open on your firewall. UDP communication is needed to all four NRPS. The NRPS also perform ICMP probes to your ORPS.

Firewall requirements for ORPS-NRPS/Support operation:

a) The organisational firewall must be configured to permit the following protocols and port numbers from the three Jisc NRPSs to the ORPS(s):

- UDP/1812 inbound and outbound (used for authentication)
- ICMP

The addresses of the NRPS:

Roaming0	212.219.190.139	2001:630:3c:c000::139
Roaming1	212.219.209.43	2001:630:3c:c001::43
Roaming2	212.219.247.59	2001:630:3c:c002::59
Roaming3	195.194.21.203	2001:630:3c:c007::203

The address of the Govroam Monitoring server:

New Support server	212.219.243.132	2001:630:3c:c003::132

b) The organisational firewall and/or ORPS firewall must be configured to allow fragmented UDP packets to pass, without any restriction on packet size, for the above servers. This is because certain EAP methods (EAP-TLS) and RADIUS server implementations result in the generation of very large packets (due to the certificate length). Such packets normally get fragmented in transit and it is vital to the RADIUS exchange that these fragments are not discarded. Whilst it may be technically possible for the default maximum RADIUS packet size to be adjusted at the Home site/IdP, due to overseas IdPs being outside UK authority and possible capability limitations of some RADIUS servers, for clarity, the Govroam policy is that any UDP packet to or from the NRPS must be permitted without fragmentation/size restriction.

If you are using EAP-TLS with Microsoft NPS, you might want to reduce MTU - see TechNet https://technet.microsoft.com/en-us/library/cc755205%28v=ws.10%29.aspx].

Testing Port 1812 firewall transit and NAT/PAP if applicable: you can verify that port 1812 is open through your firewall and any NAT/PAT translation (if applicable) is working by using the PAP authentication test on the Support server together with packet capture on your RADIUS server (eg tcpdump for linux/BSD/unix or Wireshark on Windows). You will also be able to see the requests logged on your RADIUS server when you run the PAP tests.

RADIUS server proxying configuration and attributes filtering

In this section:

- Addition of NRPS as RADIUS clients
- Configure Realm Handling, Proxying and Load Balancing
- FreeRADIUS Example Configuration - proxy, client and foreign realm handling with unlang
- Testing your Configuration - shared secrets check; authentication against local database; remote authentication
- Configure Peering with orther RADIUS servers on your network
- Configure Attribute Filtering

- Configure Injection of Operator-Name Attribute (FreeRADIUS, Radiator, Aruba ClearPass, latest Cisco ISE only)
- Configure Rejection of Malformed Usernames
- FAQs/Resources

Configure Peering with NRPSs

This step is to complete the peering of your ORPS with the NRPS by setting the NRPS as clients of your ORPS

To complete the process of peering your ORPS with the NRPS you must add all four NRPS as RADIUS clients on all of your ORPS systems (hint - edit clients.conf and proxy.conf files). Roaming0, 212.219.190.139/2001:630:3c:c000::139, Roaming1 212.219.209.43/2001:630:3c:c001::43, Roaming2 212.219.247.59/2001:630:3c:c002::59, Roaming3 195.194.21.203/2001:630:3c:c007::203 must have full authentication passes - allowed as clients on your ORPS.

If you use hostnames rather than IP addresses in your proxy configuration (FreeRADIUS: proxy.conf) it is recommended that you add the hostnames and IP addresses of the NRPS to the hosts file rather than relying on your ORPS doing a DNS lookup. This eliminates one potential issue - and ensures that the ORPS are able to send auth requests even if there's a problem with DNS.

The NRPS clients configuration must be set to use UDP ports 1812 (authentication). The NRPS will not listen on anything other than the proper RADIUS ports 1812.

The shared secrets with the NRPS are generated by Jisc.

Accuracy is essential when transcribing the shared secrets to the configuration files. It should be remembered that these are used independently to validate and encrypt client (NRPS remote authentication) and proxying (visitor authentication forwarding from ORPS) connections. An error in one of the shared secrets can lead to confusing problems such as i) remote authentication working whilst visitor authentication fails ii) unreliable performance due to authentication failure occuring when one NRPS is utilised whilst successful authentication is achieved through the others.

The following applies to Microsoft NPS implementations only. When setting up the NRPS as clients in NPS it is essential to check that the Vendor Name for the NRPS is set to ‘RADIUS standard’ and not ‘Ascend Communications’ in the NPS/RADIUS clients and servers/RADIUS clients configuration tree in the Server Manager. Open Server Manager, navigate down Roles/Network Policy and Access Services/NPS/RADIUS Clients and Servers/RADIUS Clients. The RADIUS clients pane will display the IP Address and Vendor Name (Device Manufacturer) that has been set. Device Manufacturer should be ‘RADIUS Standard’.

These instructions and the background to this requirement are described in the following Jisc Advisory:

Jisc Advisory: MS IAS and NPS Operator-Name RADIUS attribute issue (Nov 2010) - notification of critical issue affecting participants that have implemented Microsoft IAS and NPS ORPS - urgent action required.

Resources:

- Govroam wiki - Radiator RADIUS Client Definition


Needs updating or is eduroam specific

- Running Govroam on NPS with Windows 2008 R2 Enterprise (SURFnet draft doc - nb contains SURFnet-specific screenshots)


Needs updating or is eduroam specific

- Govroam.org wiki - FreeRADIUS Client Definition


Needs updating or is eduroam specific

- 'FreeRADIUS Beginner's Guide' book by Dirk van der Walt; Packt Publishing ISBN 978-1-849514-08-8

Configure Realm Handling, Proxying, RADIUS server timeouts and Load Balancing

This step is to configure your ORPS to handle auth requests originating from your network APs/controllers: forwarding Access-Requests from Visitors to the NRPS and (if applicable) forwarding Access-Requests from local users to your local authentication system.

The next stage is to configure the handling of RADIUS Access-Request packets from your network NAS systems (APs, WLCs and [if you support wired .1X connection] switches) by your ORPS. The aim is to handle Access-Request packets arising from your users authentication requests locally while Access-Requests arising from visiting users need to be forwarded to the NRPS servers. How you go about achieving this is dependent on the RADIUS platform you have deployed. FreeRADIUS and Radiator use unlang script language/PERL and in the case of FR, virtual servers which are dedicated to particular tasks and which can be tuned for best performance, whilst Microsoft NPS and Cisco ISE require policies to be defined and configuration carried via GUI.

Authentication of your own users should be considered as a separate logical process from Access-Request packet handling/'proxying'. This is covered later in section_13.

To save having to revisit this part of your configuration at a later stage, it is worthwhile tackling the issue of dealing with badly-formed usernames during this setup stage. Due to the huge number of users of Govroam and explosive growth over recent years, this is an important topic. Dealing with badly formed usernames applies to both local authentication of your own users and forwarding of auth requests for visitors. The object of filtering invalid realms is covered in the separate advisory document Filtering of Invalid Realms. How put this into practice with FreeRADIUS and for Microsoft NPS the Microsoft NPS 2008R2 config to avoid bad usernames flooding NRPS document and in the

govroam_nps_implemention_guide to be published shortly.

If using FreeRADIUS it is recommended you review our FreeRADIUS Demystified seminar material.

 Needs updating and/or is eduroam specific

[Configuration will include editing your proxy.conf file to define your local realm and editing the authorize section of radiusd.conf to program the proxying logic.] When setting up a FreeRADIUS server we'd recommend you run the server in full debug mode (freeradiusd -X or radiusd -X depending on whether it was installed by APT or from source) to enable you to see exactly what is going on for each packet and the decisions/checks the server is making as you develop the configuration.

How requests are handled and how different RADIUS server modules should authenticate and authorise the users must be configured.

Points to consider:

1. It is a requirement that ALL users (home users and visitors) authenticating via Govroam MUST have a realm component in their username (ie must be of the form 'userID@holby.nhs.uk') and that the Visited site realm handling logic drops any authentication request without a realm name in the outer id. This is to avoid a situation where your users have used a simple username eg. 'fred' to authenticate whilst connecting to Govroam at your organisation and then find that they cannot gain authentication when visiting another Govroam site. The problem would be that the Visted site ORPS will not recognise the user name and should drop it, but even if it did forward the Access-Request to the NRPS, the NRPS will not know where to forward the request to and so will drop it, returning an Access-Reject including explantory text. Do NOT permit authentication based on a simple username - insist that the username contains @realm.
2. Consideration should be given as to how both “outer” stage 1 identities and “inner” stage 2 identites are handled. You should not permit proxying of inner ID off to other organisations in cases where the inner ID realm is not your organisation - such authentication attempts should be allowed to fail. (E.g. Your RADIUS server handles an authentication request for outerID user@holby.nhs.uk, but during the auth process encounters an innerID of user@holby.nhs.uk - your ORPS must drop this auth request).
3. It is essential that your ORPS does not forward an authentication for a user from your own realm or a sub-realm to the NRPS. That would create a potential authentication loop as the NRPS would rightly return the request to your ORPS. Because such authentication loops are highly resource-hungry this situation would create a threat to the Govroam service. The NRPS have anti-auth-loop logic which drops such loop-forming requests, which protects against this threat - but please note that sending auth-loop triggers are explicitly prohibited by the Technical Specification.
4. (Advisory applicable only to FreeRADIUS and Radiator) - it is possible to set up your ORPS to be too “open” with regard to forwarding authentication requests, which can make interpretation of logs very difficult. A unsatisfactory situation can arise if your ORPS is configured to forward requests based on inner identities in addition to forwarding based on the mandatory outer ids. The default on FreeRADIUS is too open and should be closed down. By default Radiator is fine, but it is possible to set up undesirable forwarding based on inner id.
5. Only error-free authentication requests should be forwarded to the NRPS. So for example if your ORPS receives a RADIUS packet with a bad EAP-Authenticator then that packet should be

dropped at your ORPS. Bad EAP-Authenticators can arise if internal NAS systems on your network (APs and WLCs) have incorrect shared secrets with your ORPS. If the NRPS receives an Access-Request containing a bad EAP Message-Authenticator, the packet will be dropped and an error entry will be made in the NRPS log. This is potentially a very serious situation since your systems could flood the NRPS with bad packets - which will result in us applying a block to your ORPS.

6. The order in which your ORPS communicates with the NRPS should be considered. Many participants are tempted to order the NRPS in the order: roaming0, roaming1, roaming2, roaming3. The effect of this would be that roaming0 becomes the most heavily loaded of the three national proxies. In order to ensure the best responsiveness for your ORPS and to help avoid overloading any particular NRPS, it is recommended that you order the NRPS in your proxy configuration randomly.
7. Load balancing of communications with the NRPSs should be set up. However the method used must be such that all RADIUS conversation in relation to any one particular authentication event is directed through only one NRPS for the duration of the conversation. Problems arise if proxy state and conversation sequence do not tally at the NRPS.
   Radiator 3.1 and up, MS NPS, Cisco ISE and FreeRADIUS 3.x all have good EAP load balancing capability, but older software, must only be used in 'fail over' mode rather than 'load balance' (ie. use fail_over in proxy.conf, not round_robin).
8. RADIUS server timeout should be set to ensure that authentication requests forwarded to the NRPS (for onwards forwarding to your visitors' home ORPS) is sufficiently long to allow a response to be provided. Bear in mind that some visitors may be from distant Govroam federations and that several RADIUS hops may be involved. A timeout of 30 seconds is recommended. So taking the example of Microsoft NPS, the following settings are suggested:
   Number of seconds without response before request is considered dropped: 30
   Max number of dropped requests before servier is identified as unavailable: 5
   Number of seconds between requests when servier is identified as unavailable: 30
9. It is essential that your ORPSs do not mark all of the NRPS as 'dead' should no reply be received from the NPRS when handing off visitors' authentication requests to the NRPSs for onward authentication by the visitors' Home ORPS. There are logical reasons why the NRPS may not reply to your ORPS and whilst you should configure fail-over between the NRPSs in case of genuine NRPS unavailability, potentially serious communications breakdown can occur if your ORPS marks the NPRSs as dead for the wrong reason.

Remember it is not the NRPS that authenticate your visitors, it is the Home sites. The NRPS simply acts as proxy and waits for a response from the Home site. It should also be noted that some RADIUS implementations (e.g. Microsoft NPS) behave in an unhelful manner if they receive authentication requests they have difficulties with. If they recieve a request for an unknown user or if the request contains an unknown attribute, rather than respond with an Access-Reject, they simply drop the request and remain silent. The NRPS keeps the connection open, waiting for a reply, tying up NRPS resources and your ORPS recieves no response from the NRPS. The NRPS do retry the remote Home server a second time, but if there is no further response, the next Home ORPS is tried. NRPSs only act as proxies, cannot act as EAP end points and so cannot formulate Access-Rejects containing reason for failure messages. They will only forward error messages returned in RADIUS packets from the legitimate remote Home site.

Since your ORPS only knows about its immediate neighbours, i.e. the NRPSs, it may appear that the NRPS has not responded to a proxied authentication request. If your ORPS marks the NRPSs as unresponsive, zombie or dead, a serious communication breakdown can develop. The problem is that the NRPS is not dead, it is simply waiting for a response from the users' home server. So if your ORPS stops talking to the NRPS it was in dialogue with, when the NRPS sends an Access-Request for one of

your roaming users and your ORPS does not respond, your ORPS will be marked as dead. (Due to hierarchical nature of RADIUS communications, the NRPS are entitled to make this decision, you OPRSs are not).

You must configure your ORPS to avoid rogue behaviour - i.e. it is essential that your ORPSs do not mark all of the NRPS as 'dead' should no reply be received from the NPRS when forwarding visitors' authentication requests. If your RADIUS server supports Status-Server (FreeRADIUS and Radiator) you should set up your ORPS to use that.

FreeRADIUS Example Configuration - proxy, client and foreign realm handling with unlang

Replace with govroam example

We have put together an example configuration of a FreeRADIUS ORPS (both v 1.1.x and 2.x) here: example FreeRADIUS ORPS configuration on Govroam Support server

No equivalent

The first section covers configuration of the NRPS servers as proxy authenticators and clients.

About a third of the way down there is script for the authorize stanza in your proxy.conf file for your default virtual server to:

1. enforce use of full userID@realm username format
2. reject bad usernames against a sequence of common error criteria, returning reason for rejection in the reply-message
3. check for properly formed usernames in auth requests and only for valid forms, detect your local realm and hand off to local realm processing
4. hand off auths for non-local realms to Govroam realm processing

Testing your Configuration

Shared secrets check. In scenarios involving multiple ORPSs, it is advisable to test each ORPS independently for correct configuration. Shared secrets can be checked by simply running a command line test on each of the ORPS. Note that whilst FreeRADIUS, Radiator and MS NPS include utilities for cleartext password based authentication methods such as PAP, this is no longer supported by the Govroam infrastructure, so please do not attempt to use radtest, radpwtst or ntradping.

a) If you have not hooked your Wi-Fi service in to your RADIUS server, the simplest test involves using a command line tool to try to send Access-Request packets to the NRPS for forwarding to the Govroam Support IdP for a test user belonging to the Govroam realm. (This is a command line variation of the standard visitor authentication simulation test - see section 12 below).

eapol_test is included in wpa_supplicant which is an opensource supplicant that can be acquired from http://w1.fi/wpa_supplicant/

The eapol_test commands would be:

```
eapol_test -c<test.conf> -aroaming0.ja.net -p1812 -s<shared secret for
roaming0>

eapol_test -c<test.conf> -aroaming1.ja.net -p1812 -s<shared secret for
roaming1>

eapol_test -c<test.conf> -aroaming2.ja.net -p1812 -s<shared secret for
roaming2>

eapol_test -c<test.conf> -aroaming3.ja.net -p1812 -s<shared secret for
roaming3>
```

See https://www.systutorials.com/docs/linux/man/8-eapol_test/

For hints on how to build the test.conf file see
https://www.systutorials.com/docs/linux/man/5-wpa_supplicant.conf/

(Radpwtst for Radiator may include PEAP/EAP alternatives to PAP for the more advanced user.)

b) If you have peered your Wi-Fi controller/AP to the RADIUS server you can simply use the test account credentials to try to send authentication requests for the user <your realm>@govroam.uk to the NRPS

Authentication tests against your local realm user database / test auth requests from remote sites In order to carry out this test you must have a test user account on your site with a valid password (eg. a local account on the RADIUS server or an account in your user database).

You can use https://utilities.govroam.uk/radtest to perform simulated tests for your users visiting other sites. You will need to create an account on your local infrastructure and use this account to test with.

CAUTION - there is a danger that auth-loops can be created, so it is essential that the local test user account is valid and that you use credentials accurately. At the end of your test session, you must check your logs to ensure that no auth-loop has been initiated.

If you (temporarily) configure the test ORPS forwarding policy to send all access-requests with realm ('@xxx') suffixes to the NRPS, then when you use 'testuser@test.yourrealm' with radtest, the NRPS will process the request and send the access-request back to your ORPS. (Nb. if you have a group of ORPSs then this request could be sent to ANY one of the individual servers since the NRPS sends to the first ORPS in its list that it finds is not busy). Nevertheless the three lines of radtest commands are useful to verify that the ORPS can talk to all three NRPS - ie that there are no bad secrets and no firewall problems! If you do have multiple ORPSs you could always turn off the other ORPSs while doing each test - which would guarantee that only the ORPS being tested would be sent the return access-request. This would verify that the ORPS under test could be reached from each NRPS in turn).

Assuming that the test account can be authenticated using PAP, the FreeRADIUS command would be:

Radtest testuser@test.your_realm <password> roaming0.govroam.uk 1812 <shared secret for roaming0>

Radtest testuser@test.your_realm <password> roaming1.govroam.uk 1812 <shared secret for roaming1>

Radtest testuser@test.your_realm <password> roaming2.govroam.uk 1812 <shared secret for roaming2>

Configure Peering with other RADIUS servers on your network

If you choose to implement multiple organisation RADIUS proxy servers for resilience or performance/load sharing, you will have to configure peering between them.

Configure Attribute Filtering

Frequently organisations make use of attributes within RADIUS packet during the Access-Request / Challenge and Accounting exchanges to check user/machine parameters or to control how users are given access to the network. Such exchanges are frequently of local relevance only and can cause problems during remote authentication attempts. Filtering of all but the most essential RADIUS attributes from the returning packets should therefore be implemented to avoid the local access point at the Visited site receiving attributes it doesn't know how to handle.

Hint, for FreeRADIUS ORPS - you can determine what attributes are being sent in Access-Request packets by running your server in debug mode or you can run radmin to see what attributes you are sending to the NRPS. Alternatively you could packet capture and then look at the packets in Wireshark.

First off though, the following is the set of attributes required (at a minimum) to support Govroam, as listed in the Technical Specification. 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
```

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

How to set up attribute filtering? Hint for FreeRADIUS ORPS sites - in your pre-proxy section activate filtering:

```
pre-proxy {

 attr_filter.pre-proxy
```

Then in attrs.preproxy set your attributes. Something like:

```
DEFAULT

 Service-Type == Framed-User,

 Service-Type == Login-User,

 Login-Service == Telnet,

 Login-Service == Rlogin,

 Login-Service == TCP-Clear,

 Login-TCP-Port <= 65536,

 Framed-IP-Address == 255.255.255.254,

 Framed-IP-Netmask == 255.255.255.255,

 Framed-Protocol == PPP,

 Framed-Protocol == SLIP,

 Framed-Compression == Van-Jacobson-TCP-IP,

 Framed-MTU >= 576,
```

```
Framed-Filter-ID =* ANY,

Reply-Message =* ANY,

Proxy-State =* ANY,

EAP-Message =* ANY,

Message-Authenticator =* ANY,

MS-MPPE-Recv-Key =* ANY,

MS-MPPE-Send-Key =* ANY,

MS-CHAP-MPPE-Keys =* ANY,

State =* ANY,

Session-Timeout <= 28800,

Idle-Timeout <= 600,

Calling-Station-Id =* ANY,

Called-Station-Id =* ANY,

Operator-Name =* ANY,

Chargeable-User-Identity =* ANY,

Port-Limit <= 2
```

Make sure you properly test any changes.

For more information on this topic see:

- List of RADIUS Attributes
- RADIUS Attributes
- RADIUS Attribute Filtering with Microsoft IAS and NPS - the role of attribtues during authentication and VLAN assignment; why do we need to configure attribute filtering; the issue with MS NPS; how to set up filtering with NPS

Needs updating and/or eduroam specific

- Attribute Screening for Access Requests on Cisco Network Access Server

Configure Injection of Operator-Name Attribute (FreeRADIUS and Radiator only)

If you are deploying a FreeRADIUS, Radiator, Aruba ClearPass or Cisco ACS v5.4, you should configure your system to inject the Operator-Name attribute, correctly formed for your organisation, into Access-Request packets forwarded to the NRPS. The background, rationale and one method of achieving this are documented in Advisory: Injection of Operator-Name attribute (Aug 2011).

Configure Rejection of Malformed Usernames

Sending Access-Request packets to the national proxy infrastructure with malformed 'bad' usernames, more particularly those with errors in the realm component, is bad practice; definitely not good-neighbourly. Due to the prevalence of misentered usernames in laptops and mobile phones and in the case of the latter, the 'auto-correct' feature of the phone software compounds this problem, the NRPS are bombarded with Access-Requests that will never result in successful authentications. Instead, the finite resources of the NRPS become tied up waiting for responses from the Home ORPS or from the Govroam.org ETLRs in the case of non-existent non-UK realms. To avoid the above situation you should configure your ORPS to drop authentication attempts by clients with bad usernames. Bad usernames are essentially those that do not conform to 'username@FQDN' - the formal description can be found in RFC 4282, which is largely correct.

To avoid the above, FreeRADIUS deployments should utilise the Policy engine. There are now numerous examples included in the FreeRADIUS config. It is also possible to avoid the above situation is described at:www.wireless.bris.ac.uk/netcomms/Govroam-realm-checks.conf.

Needs updating and/or eduroam specific

For Microsoft NPS and IAS this is described at: Microsoft NPS 2008R2 config to avoid bad usernames flooding NRPS.

NB. There is nothing that can be done at present to avoid the RADIUS infrastructure from being hit by Access-Requests from users who have left their organisation but still have Govroam credentials configured in their devices. User education to remove Govroam configuration from devices when they leave is the best current solution.

Resources/FAQs

- Complying with the Technical Specification
- Govroam.org guide: Setting up FreeRADIUS server for Visited service
- Advisory: Filtering bad realms from auths sent to the NRPS

Missing

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

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, Radiator supplies many example configuration file snippets and templates.

eg ntlm_eap_multi.cfg which 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.

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).

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.

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

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

Needs updating and/or eduroam specific

How do I change the IP address of our ORPS? (Is there a procedure we need to go through?)

Email govroam@jisc.ac.uk and make the request.

Wi-Fi Service and Establishment of a VLAN/Network Service for Govroam

- Govroam Wi-Fi service
- The steps involved in establishing an Govroam Wi-Fi service are:
- Enabling 802.1X on your Access Points or Wireless LAN Controllers
- Peering APs/WLC with your ORPS (ORPS are RADIUS servers to APs and APs are RADIUS clients of ORPS)
- Set up radios and wireless LAN - RF bands to be used for each standard, define WLANs, enable WPA2/AES cipher
- Setup Govroam SSID
- Govroam VLAN setup
- Configure authenticated user connection policy - VLAN connection/dynamic VLAN assignment
- Tune EAP timers, RADIUS server timeout and other WLAN parameters

Most organisations provide Govroam over a Wi-Fi service although Govroam may alternatively or in addition be provided over wired infrastructure. Wi-Fi is typically the 'front-end' by which most users would prefer to connect, since this supports the laptop, tablet and smartphone devices that are most popular with users.

Many organisations have used the deployment of Govroam to simplify their wireless network offering. This can result in reduced management overhead and improved overall Wi-Fi performance and can be achieved by combining Govroam as the primary ESSID with multiple dynamically assigned VLANs as described below, together with a further small number of ESSIDs e.g. for an open captive portal network for first time users to provide access to device setup utilities or for a guest network for non-Govroam visitors.

To establish an Govroam Wi-Fi service, you need to configure the organisation's APs to broadcast the Govroam SSID, the APs need to be set to use 802.1X/AAA-RADIUS-authentication and be defined as clients of the RADIUS server. Then the APs need to be configured to forward authentication requests from the Wi-Fi devices associating to the Govroam SSID to your RADIUS server(s). Upon receipt of an validated authenticated request (an Access-Accept) the APs must connect the device to your Govroam network, described below.

If you want to use dynamic VLAN assignment as described below (assigning users to specific VLANs based on information received from the RADIUS server) then the APs must be configured to do this. (Other activities performed by the APs include exchange keying material (initialisation vectors, public and session keys, etc.) with client systems to prevent session hijacking).

Resources:

- Govroam.org wiki - Wi-Fi network set up guide for implementing Govroam Visited services (highly recommended - very thorough!)

Needs updating and/or eduroam specific

- Using Govroam as the single primary SSID

 Missing

- Cisco WLCs Wi-Fi tuning tips for Govroam

Govroam network

Visited organisations must implement one (or more) dedicated network/VLAN(s) to provide Govroam network services. All Govroam networks must comply with the Govroam Tech Spec (access to the Internet permitting use of (at least) the defined key ports and protocols - see Firewall section). Any Govroam network/VLAN must not be shared with any other network service, including eduroam. Authenticated Visitors must be connected to such an Govroam network service.

Most participating organisations permit their own users to connect via the organisation's Govroam Wi-Fi service. If this is not permitted, this must be clearly stated on the organisation's Govroam Service Information web page. Organisations may connect local users to the mandatory Visitors' Govroam network service, but alternatively may connect them to a more appropriate local network. This can be achieved through 'dynamic VLAN assignment' (which is the more efficient alternative to the fixed SSID-VLAN mapped solution). Such local networks may be used to for example satisfy the following requirements:

- provide access to local resources that the organisation wishes to be accessed only by its own users/specific groups of users
- provide a security environment required for local users/specific groups of users
- enable local users connecting their own personal devices to be connected onto an 'untrusted network'
- provide a remedial network environment for devices requiring AV updates, OS-patches etc.

Detailed information about how to set up dynamic VLAN assignment is beyond the scope of this guide, but essentially involves configuring your RADIUS server to return a value in the relevant attribute in the Access-Accept based on the policy you define for the particular user or user-group. The AP needs to be configured to act upon the attribute value and to connec the device to the appropriate VLAN. There are many guides available on the Internet, one of which is Allied Telesyn's How To user 802.1X VLAN Assignment.

Nb. The minimum set of open ports and protocols for Govroam network services defined in the Govroam Tech Spec does NOT apply to non-Govroam network services that a participating organisation may choose to connect local users to.

Requirements for Govroam network/VLANs:

- The Wi-Fi service that connects to the Govroam network service must use a broadcast SSID of 'govroam' (which must be lowercase)
- DHCP must be employed to allocate IP addresses
- Only IEEE 802.1X is permitted for the Govroam network; no form of WRD/captive portal is permitted, although you may implement this on other networks such as device setup and remediation networks

- IEEE 802.1X NASs must support symmetric keying using keys provided by the Home organisation within the RADIUS Access-Accept packet
- Only a single user is permitted per NAS port except where 'thin client'/controller-based systems are employed
- IPv4 addresses must be allocated to visitors using DHCP
- The IPv4 addresses allocated to visitors and the corresponding MAC addresses must be logged
- NAT address mappings, if used must be logged
- Routing of IPv6 on the Govroam visitor VLAN ideally should be supported
- NAT is permitted
- WEP must not be implemented on the Govroam Wi-Fi service that connects to the Govroam network service
- TLS interception proxies/filters must not be employed on the Govroam network service for visitors

Visited organisations may implement IPv4 and IPv6 filtering between the visitor VLAN and other external networks, providing that this permits the forwarding protocols detailed in the Firewall Configuration section.

Resources:

- Govroam.org wiki - Wi-Fi network set up guide for Visited services - Aruba, Cisco, Meru, Trapeze, wired


Needs updating and/or eduroam specific

- Govroam.org wiki - Configuring request forwarding in FreeRADIUS (proxy.conf)


Needs updating and/or eduroam specific

- Govroam Technical Specification
- Deploying MS IAS with VLANs


Needs updating and/or eduroam specific

Firewall Configuration to Support Govroam Network Service

If not done already, your organisational firewall must now be made ready for the Govroam Visitors network service.

An important aim of Govroam is to provide visitors with unimpeded access to the Internet, not least

because this maximises the probability of a visitor's applications working as expected. The Tech Spec therefore requires that at least the core list of protocols listed in the talble below must be permitted. You may of course open additional ports and protocols if your local policy is more liberal.

Note, if member organisations wish to absolutely ensure that their own users, when roaming, have or a wider range of ports/specific additional ports available than the minimum listed, they could provide their users with a (supported) VPN service through which the home site could control the availability of required ports and protocols.

Similarly, the Visited service providing organisation need only comply with the list for their Govroam visitor network. If you connect your own users (through your Govroam Wi-Fi service) to an alternative network service more appropriate for local users, you are not required to adhere to the minimum list (and you may be more restrictive or more open).

One approach worth considering is to offer a fairly open Visitied service network with just the ports and protocols suggested in the following document blocked and also SMTP/port 25 blocked https://community.ja.net/library/janet-services-documentation/blocking-lan-service-ports.

 Needs updating and/or eduroam specific

Your own users when at home could be connected to a network service compying with your policy for local users.

Mandatory Open Ports and Protocols:

Passive (S)FTP:	TCP/21	egress and established
SSH:	TCP/22	egress and established
IPv6 Tunnel Broker Service:	IP protocol 41	egress and established
PPTP:	IP protocol 47 (GRE) and TCP/1723	egress and established
ESP:	IP protocol 50	egress and established;
AH:	IP protocol 51	egress and established
HTTP:	TCP/80	egress and established
POP:	TCP/110	egress and established
NTP:	UDP/123	egress and established
IMAP4:	TCP/143	egress and established
IMAP3:	TCP/220	egress and established
LDAP:	TCP/389	egress and established
IMSP:	TCP/406	egress and established
HTTPS:	TCP/443	egress and established
ISAKMP: and IKE:	UDP/500	egress
LDAPS:	TCP/636	egress and established
SMTPS:	TCP/465	egress and established
Message submission:	TCP/587	egress and established
IMAPS:	TCP/993	egress and established
POP3S:	TCP/995	egress and established
OpenVPN:	UDP 1194 and TCP 1194	egress and established
Citrix:	TCP/1494	egress and established

SQUID Proxy	TCP/3128	egress and established
RDP:	TCP/3389	egress and established
IPv6 Tunnel Broker NAT traversal:	UDP/3653 and TCP/3653	egress and established
IPSec NAT traversal:	UDP/4500	egress and established
VNC:	TCP/5900	egress and established
AFS:	UDP/7000 through UDP/7007 inclusive	egress and established
HTTP Proxy:	TCP/8080	egress and established
Cisco IPSec NAT traversal:	UDP/10000 and TCP/10000	egress and established

You may have additional ports and protocols open as permitted by your local policies.

The above list is subject to change, so you should refer to the current published Govroam Technical Specification, which provides the definitive listing.

RADIUS server configuration for Home service - interoperation with user database

Configure Authentication of Preferred EAP Types

Home organisations must configure their RADIUS server (eg.edit the eap.conf file) to authenticate one or more EAP (Extensible Authentication Protocol) types as specified in the Technical Specification.

Interoperation with User Database

For each home realm authentication request handled by the IdP, the RADIUS server generally has to interrogate the user database (LDAP, NDS, AD). The interoperation of the RADIUS server with the backend user database is often the most problematic part of implementing 802.1X. Whilst there are a number of well known techniques and software combinations, since each institution 's environment is unique, detailed guidance about this is beyond the scope of this overview.

However, for FreeRADIUS with LDAP based systems, the auth handling flow is as follows: after the prefix module has run, the 'Stripped-User-Name' attribute gets populated with the userID part of the username (e.g. 'a123467') - you then use that in your LDAP configuration (ie %{Stripped-User-Name}) with the relevant CN/DN/ON that you require in LDAP.

Again, when setting up a FreeRADIUS server we'd recommend you run the server in full debug mode (freeradiusd -X or radiusd -X depending on whether it was installed by APT or from source) to enable you to see exactly what is going on for each packet and the decisions/checks the server is making as you develop the configuration.

A word on the format of user names: when migrating to an 802.1X authenticated network, it is often tempting to permit simple usernames to continue to be authenticated rather than requiring a full username including a realm element to be used. Since an Govroam username must include a realm component, the Tech Spec now requires that the username should always include the realm

component, even for Govroam networks for local users only and for users who might be thought to not roam to other Govroam sites.

It is particularly important to not permit simple usernames to be used in single-SSID Govroam networks where 'Govroam' is used for both guest users and local users.

By requiring that the full 'user@organisation.uk' type credentials are used, you can ensure that the same credentials are used by users both on the home network and when roaming. Thus problems associated with use of incorrect creadentials can be avoided. For the user, there is no confusion and after the first time that the credentials are entered into the supplicant, there is no additional work involved resulting from the adoption of this policy.

Configure RADIUS server to reject PAP requests from the NRPS

PAP is useful to have configured against a local test account during the early stages of service implementation. However, once you have used it to test port 1812 transit and NAT/PAT if applicable, since there will be no production PAP traffic, you should confgiure your RADIUS server to reject any PAP requests coming from the NRPSs.

Configure load balancing if deploying multiple RADIUS servers servicing your WLAN

If you are deploying multiple RADIUS servers to service your WLAN, think about how you are going to share the load evenly between these and your failover mechanisms.

A note on working with usernames in Microsoft NPS Windows 2008R2

Many organisations implement Govroam in an existing MS Windows network environment where usernames are stored in AD in a simple userID form without a realm component (or in some cases the realm component doesn't match the Govroam realm, e.g. Govroam realm = @holby.nhs.uk but AD realm = @ad.holby.nhs.uk). For Govroam authentication, usernames must be in the form userID@realm, therefore a means must be found of presenting the username in a form that can be successfully authenticated. (In the mismatching realms case, the Govroam realm needs to be made authenticatable). In IAS and earlier NPS versions, a perfectly workable solution has hitherto been to simply strip the realm component by using for example the find-replace rule in the Connection Request policy which is the standard Find “(.*)@(.*)” Replace “$1”. This however is no longer possible in later versions of NPS.

In NPS Windows2008R2 and later, whilst you can implement the above, the results is authentication fails even though the actual realm stripping seems to work - the stripped username is found in the AD, but still the authentication fails, (almost as if the password is wrong). Interestingly you could even strip the original .ac.uk type realm component (e.g. @holby.nhs.uk) and replace it with a local one (e.g. @ad.holby.nhs.uk or @camford.local) that matches a valid username in AD, but the result would be the same.

This is because in Windows 2008R2 Microsoft decided to change the way that NPS deals with realms. In 2008R2 a stripped realm no longer passes EAP security requirements and thus the stripping of a User-Name always results in an authentication failure.

The fix for this is to do one of the following:

1. Configure the realm stripping rules on the front-end NPS server to modify the identity in the Access-Request and then forward the request to a second NPS server for authentication OR just send the Access-Request to a second (earlier release) Microsoft RADIUS server (older NPS or even ancient IAS box) to do the stripping and authentication.
2. The recommended solution is to add your Govroam realm as another global UPN to your AD so you don't need to strip the realm in the first place.
3. Use a different RADIUS server platform!

Set up logging

Logging on the ORPS must be set up in accordance with the Technical Specification. All transactions with the NRPS, including some mandatory attributes, must be logged and records held for at least 3 months, with a recommended maximum of 6 months (subject to your own policies).

RADIUS Accounting

Please do not send RADIUS accounting to the Govroam NRPS. Jisc's firewall will block any port 1813 traffic.

Resources:

- Technical Specification
- Complying with the Technical Specification


Needs updating and/or eduroam specific

- Govroam.org guide: Setting up Various RADIUS servers for Home service


Needs updating and/or eduroam specific

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


Needs updating and/or eduroam specific

Govroam Authentication Tests

Tests available to Govroam administrators at participating organisations from the RadTest web site enable testing on demand of :

1. authentication of one of your users visiting another organisation, using authentication protocols: PAP, EAP-PEAP, EAP-TTLS.(*)
2. authentication of a user visiting your site from another organisation (ie that your ORPS is forwarding RADIUS packets correctly and handling attributes within RADIUS-challenge/response etc. packets ok).(*)

(*) EAP-TLS - test facilities are not available at present due to the complexities relating to the digital certificate requirements (clients require unique server and client certificates).

How to use the tests:

1. The test user account should be created in the organisation's user database that is authenticated against by Govroam. This should allow at least five failed authentication attempts without being locked. Nb The test account credentials will only ever be known to you.
2. Go to the RADIUS Testing web site and enter the credentials of your test account.

The available test function is:

- Remote User Authentication Tests. To check that one of your users at a remote site can be authenticated by your systems.

EAP-PEAP authentication test - PEAP is commonly used for 802.1X authentication. This option will work for most RADIUS servers. Some servers, e.g., Radiator, may require PEAPv1.

The options are:

PEAPv0-MSCHAPv2

PEAPv1-MSCHAPv2

TTLS-PAP

TTLS-MSCHAPv2

Remember that when testing a user from your own organisation authenticating using your 802.1X network, if the user can be authenticated on your network, then provided that proxying works, the user will be able to successfully authenticate at any compliant visited organisation.

Visitor Authentication Simulation Test

Govroam Monitor of ORPS

Testing a new ORPS within Govroam Infrastructure before bringing it into production use

RADIUS server log keeping and interpretation of logs

It is a mandatory requirement of the Govroam Technical Specification that participating organisations keep RADIUS logs of authentication traffic.

It is strongly recommended that Govroam System Administrators make it routine practice to inspect their RADIUS logs in order to detect any abnormalities and hidden problems.

Clarification of Policy and Tech Spec Wording - Visitor Activity Logging


Needs updating and/or eduroam specific

Hint for FreeRADIUS ORPS: the default main logfile (radiusd.log), which is configured in the main radiusd.conf file and which logs OK messages etc., is rather basic.

It is recommended to use linelog module for logging - this will enable you to log any of the attributes present in packets. And if you also call linelog in the inner-tunnel authentication phase, attributes relevant to local authentication of your own users can be logged such as EAP type. Rather than fill up your ORPS with log files you can also push logging off to a remote syslog server. And FR 3 includes more funky NOSQL/Logstash stuff.

FAQs:

1. Can you clarify the Policy/Tech Spec on vistor logging?

See - Clarification of Policy and Tech Spec Wording - Visitor Activity Logging

1. Using the RADTest facility results in errors in our FreeRadius log due to use of null value outer user name by the Govroam Test. Why is this and what's the solution?


Not applicable unless some functionality is added

The log error is due to the server using an outer user name comprising just the realm name for the Test. This conforms to the correct RFC format for anonymous outer identity, in accordance with RFC 4282:

Omitting the username part is RECOMMENDED over using a fixed username part, such as “anonymous”, since it provides an unambiguous way to determine whether the username is intended to uniquely identify a single user.

The Govroam test used to use anonymous@realm, however feedback from several organisations led us to adopt the correct RFC format.

ORPS shouldn't be acting on the outer identity unless you really need to - this value is easily set to be

whatever value you want and therefore must not be used to authorise. The solution is to add a simple addition to the sql.conf which remove this from logging etc. the inner ID should still be accounted and logged.

1. The NRPS are only testing one of our ORPSs using the test account configured on the Support server, why is this?

Jisc has set up a system to monitor the RADIUS request handling status of Home organisations, ie. that an ORPS is operational. This is done using the test user account that participating organisations set up on the Govroam Support server.

In your RADIUS logs you are seeing a single NRPS using the Govroam Support test account to check the service status on just one of your ORPS. The reason for this is that the RADIUS check is being launched from the support site and goes via the NRPS. So a NRPS that can handle the request will only pass the request through to the first working ORPS at your site. This validates that your site is currently able to handle Govroam RADIUS requests but does not check that ALL of your ORPS are alive.

The servers can be checked for network connectivity by PING but the only way to check RADIUS would be to allow a direct Support Server to ORPS RADIUS link. This is deemed unacceptable and would invalidate the Govroam check - as we really need to monitor how the NRPS see the ORPS. Monitoring of the status of the ORPS system (be they load balanced, failover or round-robin constructed) is down to the individual organisations.

Monitoring your own service

A monitoring system should be set up to ensure that you are aware that your Govroam system is operating satisfactorily and that your OPRS is communicating with the NRPS (and with any ORPS within your Federation, if appropriate). Nagios is often used for this purpose (and this is what Govroam uses to monitor the availability of participants' authentication systems).

Participants are permitted to use the Govroam visitor authentication simulation test for their own monitoring solutions, but if you do so you must configure any such solution to only query the visitor authentication simulation test service at intervals exceeding 5 minutes.

If your RADIUS solution supports server-status (FreeRADIUS and Radiator), you should employ this method to check that your ORPS can successfully communicate with the NRPS (and that the NRPS are responsive).

Setting up User's Devices/'Onboarding'

One of the hurdles to be overcome in a successful 802.1X institutional deployment is getting the devices of your users setup to work with Govroam. You may have chosen to utilise a third party 802.1X supplicant or to reply on the built in OS supplicant or you may want to support both and/or a variety of EAP methods. Whichever policy you adopt, you are faced with three challenges:

1. Not all devices, operating systems and supplicants are equal with regard to their 802.1X capability
2. Getting requisite third party supplicants and certificates to devices and installed
3. Getting devices properly set up and optimised, including possibly removing legacy configurations and setup SSIDs

Devices and operating system supplicants that are compatible with Govroam

See the GEANT wiki table: Devices that are compatible with Govroam To a large extent we are at the mercy of product developers to properly implement 802.1X supplicants for their products and OSs.

Distribution of third party supplicant software and certificates (where applicable)

Once you have decided on the supplicant of choice and the necessary EAP settings there remain potentially two major operations:

Distribution of third party supplicant software - if you have decided not to rely on built in operating system supplicant.

Getting the user's device Properly set up - auto-configuration tools

Configuration of this supplicant software - a large proportion of users are either relucatant / not up to the job of correct configuration of the software. Expecting users to correctly configure supplicants, whether native or third party, is being somewhat optimistic. It is essential that the setup should include configuration of the client for checking of the ORPS certificate! (Without this check, users are susceptible to credentials harvesting attacks.) Automating this process serves to help both the end user and IT Services, since the burden of fixing misconfigured machines can be eliminated.

There are now at least three tools which make the whole undertaking much more manageable:

- Rukus Cloudpath - commercial and therefore incurs a cost, but it does support Windows, MacOS, Ubuntu, SecureW2, and OpenSEA Xsupplicant supplicants. We've put together a detailed case study describing why and how Bristol University rolled out configuration of Windows native supplicant to its users using CloudPath XpressConnect: Automated 802.1X set-up for Govroam users at Bristol University using Cloudpath.
- Govroam Configuration Assistance Tool (CAT) - a tool that builds configuration installer programs which can be downloaded and distributed under the control of the participating organisation's Govroam sys admin (e.g. via the Govroam service information web page) or downbloaded directly by individuals. To use the Govroam CAT tool (developed through the Geant Govroam confederation), you need to have a compliant Home service and an invite token. To get a invite token email govroam@jisc.ac.uk and ask for a CAT token. 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. You can use social media credentials to activate the account or the eduGAIN federated access. The CAT is fully documented at https://wiki.govroam.uk/doku.php?id=jisc:govroam_cat_documentation_for_organisational_administrators

FAQs:

- How do I configure Windows to work with 802.1X?

Details of all aspects of setting up the client and using Govroam are included in the User Guide.


Need windows 7 and 10 guides.

- Why is it important for the supplicant to be set to check RADIUS server certificate?

For answers to this and to understand server certificate validataion see Kevin Koster's presentation at NWS38 Nb. The Jisc Certificate Service CA chain is now USER Trust - UTN-USERFirst-Hardware - TERENA SSL CA.


Needs updating and/or eduroam specific

Q.A. Test of your Govroam implementation

Govroam is a federated service and as such relies on all participants to offer high quality operational services - the Technical Specification is in place to try to ensure this, but by its federated nature there is a degree of trust that participants will implement it faithfully. There is at present no national accreditation process, so we rely on participating organisations to test their implementations thoroughly themselves. An unreliable or badly configured service reflects badly on the rest of the Govroam world and brings the service into disrepute.

Your network should not broadcast the Govroam SSID until you have an operational service, ie you can tick off compliance to the requirement of the Technical Specification and the following tests can be passed. You can then say with confidence that you have a working service.

govroam_technical_specification_summary_of_requirements_checklist - tick box list to enable you to verify compliance of your service


Govroam version required: https://community.jisc.ac.uk/groups/eduroam/document/eduroamuk-technical-specific

ation-v14-summary-requirements-checklist

govroam_tech_spec_summary_of_recommendations_checklist - tick box to help you assess your implementaton of recommendations

Govroam version required: https://community.jisc.ac.uk/groups/eduroam/document/eduroamuk-technical-specification-summary-recommendations-checklist

ORPS - NRPS Communication Test ICMP check - the reachability of each ORPS must be verified individually. All ORPS must be reachable by UDP and ICMP/TCP (and so your firewall must be configured accordingly) and must be peered with the NRPS and handle RADIUS traffic correctly to support authentication.

Authentication Test - Authentication check from each NRPS to your realm. This tests authentication via the first available ORPS at your realm. This verifies proper configuration of NRPS 'clients' and realm handling on your ORPS

- EAP Authentication Check - access-accept for roaming0
- EAP Authentication Check - access-accept for roaming1
- EAP Authentication Check - access-accept for roaming2
- EAP Authentication Check - access-accept for roaming3

Visited Organisation - Visitor Authentication Simulation Test - to verify that authentication attempts by visitors to your service will be forwarded to the NRPS, the visitor authentication simulation test, should be run where applicable.

- Visitor Authentication Simulation Test - success

Peering Configuration check (verify ALL shared secrets) - The basic authentication check above only tests authentication via the first available ORPS at your realm. In cases where there are multiple ORPS, the client peering of each ORPS for each NRPS must be also be checked individually. Similarly the visitor authentication simulation test only checks authentication via one of the NRPS to the 'Govroam.ac.uk' realm. Run utilities such as radcheck to verify shared secrets for all ORPS-NRPS combinations, client and proxy.

- to verify proper configuration of all four NRPS 'proxy' settings on your ORPS and in multiple ORPS deployments to verify NRPS 'client' configs: radcheck / radpwtest / ntradping tests - ok for each ORPS/NRPS combination

Correct Realm Handling by ORPS (anti-auth-loop) - to reduce user authentication/misconfiguration problems and eliminate the danger of your ORPS marking the NRPS as dead due to our ORPS-NRPS authentication loop prevention logic. The test usernames listed below should be applied to a client on your network and you should check that your ORPS handles realm names correctly and does NOT proxy the authentication attempts up to the NRPS. Such misbehaviour could potentially initiate an 'authentication loop' since logically the NRPS should send the auth-request back to your ORPS and the ORPS would then erroneously send the request back to the NRPS again - causing a never-ending authentication loop as access-requests have no time-to-live limit. This would be a serious situation leading to a loss of service.

To prevent this, the NRPS have anti-authentication loop logic which will drop the misdirected access-requests if your OPRS does forward such usernames. However, since your ORPS will get no reply from the NRPS there is the danger that your ORPS will mark the NRPS as dead - leading to it not forwarding valid access-request packets for a period of time and causing authentication problems. It is therefore important that your ORPS handles username variations correctly.

ORPS username handling tests ('realm' stands for your full realm name eg. 'myorganisationname.uk'):

- testuser@realm@other(egCAauthrealm) - handled locally and NOT forwarded to NRPS
- testuser@UPPERCASErealm - handled locally and NOT forwarded to NRPS
- testuser@validsubrealm.realm - handled locally and NOT forwarded to NRPS
- testuser@realm - handled locally and NOT forwarded to NRPS
- invalidtestuser@realm - rejected locally and NOT forwarded to NRPS

The following section focusses on expands on invalid User-Name (ie those that do not conform to the Network Access Identifier standard).

Username Handling Conformance Check - of particular importance in deployments where a single SSID 'Govroam' is implemented at an orgnisation, usernames MUST be in the form user@myorganisationname.uk (.net and .org.uk are also acceptable as is .subrealm.uk etc.) This ensures that users are able to utilise Govroam in a seamless manner when they travel.

The following test usernames should be applied to a client on your network and you should check that your ORPS drops them without authentication against your user database or forwarding to the NRPS:

- testuser (no realm name component) - authentication should be dropped (User-Name MUST contain '@')
- testuser@@anyrealm (contains two '@') - authentication should be dropped (User-Name MUST NOT contain '@@')
- test user@any realm (contains spaces) - authentication should be dropped (User-Name MUST NOT contain ' ')
- testuser@.anyrealm (starts with a dot) - authentication should be dropped (User-Name realm MUST NOT start with '.')
- testuser@anyrealm. (ends with a dot) - authentication should be dropped (User-Name realm MUST NOT end with '.')
- testuser@myorganisationname..ac.uk (contains double dot) - authentication should be dropped (User-Name realm MUST NOT contain double '..')

Govroam Information Web Site - you must have an information web site as detailed in the

Tech Spec

and described in section 18 below promoting Govroam at your organisation

Internal link

.

- Govroam information page on organisation web site - yes

Promoting Govroam at your organisation

There are three key elements to promoting Govroam at your organisation:

A dedicated 'Govroam service information' page or Govroam section on the Wi-Fi service page on your organisation's web site. This must provide Govroam users with the key information to enable them to use the Govroam service at your site. This is mandatory requirement of the Tech Specification. A content guide is available.

Needs updating and/or eduroam specific

Advertising the locations at which Govroam is available and raising general awareness of Govroam in your organisation.

Providing information to freshers and training if necessary to your own users about the service.

Govroam service information web page

It is a mandatory requirement of the Technical Specification that Visited organisations publish information on their web site page for visitors about how to use Govroam at their site. You must update the URL of your Govroam information page on the Govroam Configuration page on the Govroam Support web site. (This enables this information to be published on our Govroam locations map pages).

Although it is not mandatory for Home only organisations to publish a 'how to use Govroam' web page, it is highly recommended that you publish such a page to provide information for your own users to help them to use the service when they roam to other sites.

For Visited organisations, the Tech Spec requires that their Govroam web page is accessible from both the Internet and from within the organisation in order to allow visitors easy access to information they may wish to refer to.

As a minimum the Visited organisation's web site must include the following:

The participant’s acceptable use policy (AUP)

Sufficient information to enable visitors to identify and access the service; the locations where Govroam is available, the Govroam Tier(s), and the SSID(s)

Information regarding any application or interception proxies that may be deployed and if this is not transparent, how to configure applications to work with the proxy

There is further guidance in the content guide.

Advertising the locations at which Govroam is available and raising general awareness of Govroam

There is a range of ready-made material published on the Govroam.org web site which you may find useful. This includes a leaflet and sticker. All you need to do is enter the country, NREN and your organisation-specific details in the pdf fields and print on a suitable medium. If you need the Jisc logo, please apply for this via Jisc service desk.

See: https://www.Govroam.org/index.php?p=media

Govroam version required. - https://www.eduroam.org/?p=media

Providing information and training if necessary to your own users on the service

We would suggest that information on how to get started with campus network services includes information about Govroam. You might want to provide an open access captive portal network service for first time users that simply provides information about Govroam, links to your preferred Govroam setup tools and guidance on how to get IT support.

Mapping App