Govroam FAQ

Onboarding

Q: We're a public sector organisation and would like to join Govroam, what are the next steps?

A: Contact govroam@jisc.ac.uk and you'll be sent all the appropriate documentation for joining.

The full boarding form needs filling out completely. It asks for contact information, information about your RADIUS servers and various other pieces of information. If you're joining as a Federation, please fill in the

Registry

document too and send it to govroam@jisc.ac.uk.

Once we have properly completed forms then we'll sort out the appropriate payments, send you an encrypted file with the shared secrets for RADIUS servers, the Govroam App, subscribe you to the support mailing lists and add your support details to our Support Matrix.

Q: We're a public sector organisation and would like to join Govroam as a Visited Only site, what are the next steps?

A: Contact govroam@jisc.ac.uk and you'll be sent all the appropriate documentation for joining.

The Visited Only boarding form needs filling out completely. It asks for contact information, information about your RADIUS servers and for a letter of consent, on corporate headed paper, from someone senior e.g:

```
"Dear Sir/Madam,

Re: Govroam

Please accept this letter as authority of behalf of <insert organisation
here> for the provision of the Govroam service over our network
infrastructure as a Visited Only site.

Your faithfully,

<Director of IT>"
```

scan it to a PDF and upload it to the form.

Submit the form back to us, and then we'll send an encrypted file with the shared secrets for RADIUS servers, the Govroam App, subscribe you to the support mailing lists and add your support details to our Support Matrix.

Q: We're a University/Third Party that wants to implement Govroam as a Visited Only service. What do we have to do?

A: There are three things to do:

1. If you've already got eduroam then take your existing configuration, duplicate the part of it related to visitors, change the 'eduroam' bits to 'govroam'. So that should cover the SSID, 802.1x setting on your wireless controllers, a VLAN to put the visitors on, an address range for them, firewall settings (same as eduroam). Then the RADIUS config should be able to send unknown realms to our NRPS.

2. Have your Director of IT (or someone suitably senior) write a brief letter of authorisation, on corporate headed paper, along the lines of

```
"Dear Sir/Madam,

Re: Govroam

Please accept this letter as authority of behalf of <insert
institution/organisation here> for the provision of the Govroam service over
our network infrastructure as a Visited Only site.

Your faithfully,

<Director of IT>"
```

scan it to a PDF and upload it through the form below.

3. Visit the Visited Only boarding form, fill it out and submit it. You will need to have the hostnames of your RADIUS servers already configured.

Then we'll send you an encrypted file with the shared secrets for our NRPS for you to configure in your RADIUS servers. We'll include a test account so that you can confirm that outgoing authentication requests work and we have a web page through which you can test incoming authentication requests. We'll sign you up to a technical mailing list and give you access to our Wiki of relevant information.

An overview of how to deploy visited-only govroam alongside an existing eduroam service:

Joint deployment presentation
(first presented November 2019)

Our technical requirements in detail:

Tech Spec V3

Technical

Q: What's the relationship between Govroam and eduroam? Do I need one to have the other or do I have to have both?

A: They're very closely related but they aren't the same and there are no dependencies either way. eduroam has been around for years in the academic sector and is mature. Govroam uses exactly the same idea and technology but is aimed at NHS, Local Government and other public sectors. JISC runs the top level RADIUS servers for both services but they are completely separate services.

Thus it's possible to have neither, either or both.

If you already run eduroam as a Home site (i.e. a University) then adding Govroam as a Visited Only site is easy (and free). Essentially you need to duplicate your wireless and RADIUS configurations and request the shared secret details from JISC. This may require separate infrastructure (normally different RADIUS server VMs) or could be done on shared systems.

It's not possible for people with eduroam accounts to authenticate using Govroam, or vice versa. We encourage sites with eduroam to run Govroam Visited Only and Govroam sites to to eduroam Visited Only, for maximum coverage.

Q: Which should I have?

A: This very much depends upon the sort of users you have at your site. The services have concepts of Home and Visited:

Home is where a user has their credentials stored/generated (e.g. a University for an eduroam user or an NHS Trust for a Govroam user. At a Home site there will be a wireless system, RADIUS servers and a credential store (e.g. Active Directory).

Visited is where the user roams to and wants to work from. A Visited site will have a wireless system and RADIUS servers.

Now a site can be one or the other, or both. And that goes for both services. (Although it would be rare to have a Home only site).

Typical scenarios:

- A University: Home and Visited for eduroam. Visited only for Govroam. A University might want to offer connectivity to NHS staff visiting from the Teaching Hospital next door.
- A Hospital: Home and Visited for Govroam. Visited only for eduroam. A Hospital could have medical students on site and want to offer them connectivity.

In both these scenerios there might be people who work for both the University and a Hospital. In which case they could have two sets of credentials or just credentials from one side. At either the Hospital or the University they could still connect with either set.

- Reseller: Visited for eduroam and Govroam. They want to be able to offer the connectivity to their customers when on their site.

So ask yourselves “What sort of users to we want to offer services to?”. If you're a public sector employer then you'd want to be Home and Visited for Govroam. If you've got academic types on site

then consider offering Visited for eduroam. If you're a University then you can offer Visited Govroam alongside your eduroam install for free.

Q: What hardware/software is required for Govroam?

A: As much or as little hardware as you want/Any RADIUS server.

A full service requires a wireless system, RADIUS and a network connection to the Internet. Assuming that you have the former and the latter then the RADIUS hardware is fairly simple. RADIUS software doesn't use much in the way of resources. e.g. A Raspberry PI running RadSecProxy could handle dozens of requests per second and would be functional for a medium sized enterprise - although not recommended! Any modern rack mount server, or a VM with a couple of CPU, a couple of GB of memory and 10GB of storage would be more than adequate for a top level RRPS or ORPS.

If you already have a RADIUS server then you may be able to configure it to act as an ORPS at no extra cost. If the software doesn't allow it, or you want to separate your services then the ORPS you add will only be handling the authentication requests destined/source to/from offsite, which will by about 1% of your total authentication requests.

As for the software - any modern RADIUS server can handle Govroam. There are no odd requirements. Having said that though, there should be a preference for servers which can handle Server Status (for resilience), CUI (Chargeable User Identity for audit), Operator-Name (for logging) and RADSEC (for the future).

If you value the service then resilience should be considered. At least two RADIUS servers at each level are recommended and three is quite common. Many RADIUS servers (and wireless controllers) offer load balancing options so hardware load balancers shouldn't be needed. The servers themselves are generally stateless and require no intercommunication.

Q: How much does the hardware/software cost to run Govroam RADIUS on?

A: Following on from the above question: between zero and a lot. If you have a spare piece of hardware, or can create a VM at no cost then installing a linux variant and FreeRADIUS would cost nothing. As would adding the ORPS capability to an existing RADIUS configuration. If you have to buy hardware then £500-1000 should cover the cost of a suitable Dell server. If you want to purchase RADIUS software such as Clearpass then you'll have to talk to a reseller as the licences can be complex. Even a reasonably sized hospital ought to be able have something for under £5,000 though. The final costs with depend on a number of factors which are site specific.

Q: What do I do with users once they're authenticated?

A: You can make this as simple or as complex as you wish. There is a minimum service level associated with govroam but it's not particularly restrictive. At the simplest level govroam Visitors to your site need a network segment separate from other users, a basic set of open ports (such as web and VPN) and some bandwidth.

Note 'govroam visitors'. If you're using govroam for your own people on your own site then you can treat them differently (put them on a VLAN/firewall context which has less restrictive firewalling or more access to local services, for example).

A common approach is to use a RADIUS attribute, set by the ORPS, to identify the user as a Visitor and set an appropriate role on the wireless system/firewall.

Q: What EAP types can we use?

A: Easy one: any. The slightly longer answer is that any data in the inner tunnel is encrypted so is completely independent of the outer tunnel. As long as the outer tunnel has the right 'routing information' i.e. the realm, then the proxying will work. Thus each site can be using a different EAP type and it should all work. The use of PEAP is very common, EAP-TLS less so but plenty of sites use it successfully.

Q: Would you be able to provide direct support with setting up and running our RADIUS system?

A: Jisc can provide a variety of different sorts of help at various levels and there are plenty of options outside of Jisc.

Jisc can:

1. Provide high level documentation covering how federated authentication works and the technical requirements
2. Work with sites during the onboarding phase
3. Offer onsite, paid, consultancy if sites are using particular RADIUS software (FreeRADIUS, radsecproxy, Clearpass).
4. Attempt to put sites in contact with Federations with suitable experience or Universities prepared to offer help.

Jisc isn't in a position to recommend external consultants or commercial third party partners, however, there are several companies who are able to offer these services and are currently doing so for both Govroam and eduroam. They should also be able to offer ongoing support.

Joining with an existing Federation has the benefits of potential significant reductions in boarding fees as well as access to people in your area and your field with existing experience of configuring Govroam.

Jisc has experience with RADIUS software such as FreeRADIUS and radsecproxy so can offer full configuration support as well as limited configuration advice on Clearpass.

Virtually all Universities have been using eduroam from many years so have significant experience and are often very willing to help others. They may not have much time to spare though and experience limited to the common eduroam RADIUS platforms, such as FreeRADIUS and Cisco ISE.

Jisc is able to provide a test account and some tools for external testing of credentials. We will work with sites until the boarding is complete and authentication works through the proxies.

Q: Which RADIUS server should we use?

A: Jisc aren't allowed to recommend particular RADIUS servers. The ones we're aware of that meet all the requirements of our Technical Spec are

- FreeRADIUS (open source, linux),
- radsecproxy (open source, linux),
- RADIATOR (commerical, linux and Windows),
- Aruba Clearpass (commerical, appliance).

radsecproxy is purely a proxy whereas the others can also integrate with data stores for authentication. Other RADIUS servers may also meet the requirements.

Q: As a Federation what process should we follow when Onboarding sites?

A:

1. For each site gather the details of their RADIUS server(s), realm(s) and a technical contact. This would include IP address(es)/hostname(s), non standard ports, any load balancing and whether they support Status Server.
2. Configure your RRPS for the above, generating suitable shared secrets. The configuration should, obviously, include the client/server information to allow communications between RADIUS servers and suitable routing of the realms.
3. Share these shared secrets and the details of your RADIUS server with the site technical contact, securely.
4. The site should then configure their end.
5. RFO should then provide Jisc with the following information about the site (This is all put onto our wiki and made available to all sites for troubleshooting, incident and audit purposes):
    1. Realm(s)
    2. Name and location of the site
    3. Name, position, email and phone number of the technical contact for the site
    4. Help desk (website, phone number, openings times) for the site.
6. The site can then test outgoing connectivity either using credentials supplied by the Federation, or the ones provided by Jisc. Incoming connectivity can be tested using the website provided by Jisc with local site credentials.
7. The site is provided with a login to Jisc's App site so that they can populate Govroam locations on a map.

This

spreadsheet

can be used as a template for the information that should be collected for sending to Jisc: (govroam@jisc.ac.uk). Use RED to indicate information to be removed, YELLOW for changes, and GREEN for new additions.

Q: How do I unpack the file sent?

A: Follow these instructions: Unpacking .tar.gpg.zip file

Q: Firewall is seeing fragmented packets from RADIUS servers?

A: If the RADIUS packets exceed the MTU size then they'll be fragmented. This normally happens only with EAP-TLS (client certificate based authentication). We have some suggestions on how to deal with packet fragmentation.

2018/05/11 13:50 · admin

For Existing Govroam Users

Q: Why doesn't the test account work?

A: Firstly, the authentication request has to be made using EAP, not just a PAP or MSCHAP request. Secondly, until Jan 2018, the Root CA on the RADIUS server at the JISC end was a generic, self-signed one, but now is signed by QuoVadis. This used to require turning off certificate checking while testing but now shouldn't. However, if you still have problems it might be worth disabling verification so see if it helps.

Q: What's this about realm filtering?

A: In an ideal world the only unknown requests proxied from one RADIUS server to another would be those for realms which exist elsewhere. In practice though, most of the unknown requests don't contain a valid realm. For instance, a Camford (camford.org.uk) RADIUS server would forward a request for the holby.nhs.uk realm upwards and it would eventually arrive at the Holby RADIUS server but it would also forward cmford.org.uk, cmaford.org.uk, camford.uk etc. See section 4.2.1 of the Tech Spec for more info.

The number of these non-valids can exceed the valid one by factors of thousands to one (mostly because of retries from the client) and can put a significant and unnecessary load on RADIUS servers. So applying rules on the ORPS to spot and remove these as early as possible is a great idea. It's impossible to catch everything but there are a few easy rules that can be implement:

1. Null realms: where the end-user hasn't put a realm in.
2. Syntactically valid realms:
    1. MUST contain at least one dot (“.”), e.g. “camford.org.uk” is OK,
    2. MUST NOT start or end with a dot, e.g. “.camford.org.uk” or “camford.org.uk.” are both invalid,
    3. MUST NOT have two or more sequential dots, e.g. “camford.org..uk” is invalid,
    4. MUST consist only of alphanumeric, hyphen and dot characters, so that's a-z, 0-9, “-” and “.”, spaces are explicitly not permitted, e.g. “camford.org uk” is invalid,
    5. following on from the previous point the realm MUST NOT start or end with a space, e.g. “camford.org.uk ” is invalid,
    6. The regex “^[^@]*@[^.]+([a-zA-Z0-9-]+\.)+[a-zA-Z]{2,6}$” should match syntactically valid usernames but it's not well tested.
3. Misspelling of your local realms. If you know that a realm is very likely to be invalid re: cmford.org.uk then filter it out too.
4. .local can be used locally but should never be forwarded on.
5. Realms with aren't ever likely to be part of the federation:

- myabc.com
- 3gppnetwork.org (plus all subrealms thereof)
- 3gppnetworks.org (plus all subrealms thereof)
- gmail.com
- googlemail.com
- hotmail.com
- hotmail.co.uk
- live.com
- outlook.com
- yahoo.com
- yahoo.co.uk
- yahoo.cn
- unimail.com

In FreeRADIUS take a look at the 'filter_username' policy which covers some of the basic cases. You will want to sanity check the tests though to make sure that they're suitable for govroam. If nothing else the file will give you a template to use when writing your own filters.

Code Snippets

Q: What value should I use in the Operator-Name field?

A: Normally it's the realm which the RADIUS server handles. If there are multiple realms then use the one which best identifies your site. The format is '1holby.nhs.uk'. The '1' is mandatory and defines the follow as a 'realm'.

Q: What monitoring should I have in place?

A: Generally that your choice and dependent on what you need from the service and what tools you have.

Options:

- ICMP (ping). The NRPS are pingable so you could ICMP for status checks and graphing of latency.
- Test account. Jisc have provided a test account and are happy for sites to use this as an 'authentication ping'. You'll need to set up your monitoring system to be able to send out EAP auth requests but command line tools like 'eapol_test', which comes with WPA Supplicant is useful for this. Monitoring systems, such as Nagios, have plugins available for RADIUS status checking.
- Some RADIUS servers, FreeRADIUS for example, have methods for extracting usage data. FreeRADIUS uses the 'Status Server' approach where a special request is sent and information returned (what and to where is configurable). Others use SNMP and have a custom MIB with the information. This approach is useful for monitoring your own servers as you're able to collect information about number/rate of authentication requests, successes and failures. Tools like Observium have built-in support for FreeRADIUS and could be used to gather from generic SNMP sources too.

- Processing of logs is a way of checking for problems. Checking for common failure messages, errors or server problems. Compiling or graphing statistics on various metrics (failed auths per realm, timeouts per server) can indicate systemic failure in certain areas. Tools like ELK can process logs, parse, collate and graph such logs.
- If you're running a Federation then you might want/need to monitor the status and history of the sites you have connected. Many of the above approach can be used with remote RADIUS servers too. Status Server, if supported, is particularly useful for this.

Q: Identities seem to have been replaced with 'anonymous@realm' or '@realm' and these aren't authenticating. What's going on?

A: EAP requests have inner and outer identities. Inner identities are something like 'fred@site.org' and the username part 'fred' is used to authenticate the user. The Inner identity is contained within an encrypted tunnel and not visible other than at the client and IdP ends i.e. the proxies can not see the Inner credentials.

The Outer identity is visible to all RADIUS servers and is sent unencrypted on the wire. It used only as a way of routing RADIUS requests around the infrastructure. The username portion is unused and irrelevant. i.e. from 'fred@site.org' only the 'site.org' portion is used, so that RADIUS proxies know where to send the request on to.

For security reasons it's strongly recommended that clients are configured with anonymous outer identities such as '@site.org' to prevent user names from being logged or being sniffed. As such it's incumbent on sites to ensure that their RADIUS servers do not insist on the outer ID matching the inner ID or that the outer ID username part is used for any aspect of authentication or routing.

To be clear, RADIUS proxies should proxy packets with outer of '@<realm>', 'anonymous@<realm>' or '<anything>@<realm>'. RADIUS IdPs should be able to authenticate based on the inner ID only.

Q: Can I use a hardware load balancer for the RADIUS servers?

The general advice is that it's not necessary and might not work anyway.

There are two issues to consider:

1. There is a shared secret between each pair of RADIUS servers (ORPS/RRPS, RRPS/NRPS) so if you have 3 RRPS and 4 NRPS then that's 12 separate communication paths each with a shared secret. How does a load balancer deal with that?
2. Whilst basic RADIUS authentications (PAP, MSCHAP etc.) are individual UDP requests which can be load balanced quite trivially, EAP uses a 12 way handshake which is stateful. Each authentication attempt has to happen between the same pair of RADIUS servers otherwise it will just fail. Thus load balancers have to be EAP-aware and configured accordingly.

Most RADIUS servers have pretty decent load balancing built in anyway so putting an extra hardware layer in place wouldn't improve resilience much, if at all.

Q: How do I configure Windows for client certificates

For proxying the Outer ID needs to be of the right format (@<realm>)

Q: Why are Zombies bad?

In RADIUS terms 'zombies' are RADIUS servers flagged as dead by another RADIUS server. RADIUS servers need to monitor the state of their neighbours to ensure that auth requests are handled. With TCP connections this could be done by simply noticing that the TCP connection fails, however with UDP this is not possible. Thus the approach is to wait a set time for a response and mark the neighbour as down (or a 'zombie') if no response is received. After another set period the neighbour is returned to the pool and the process starts again. Generally it only takes one such failed response for a server to be marked as a zombie. The response timeout is normally 30 seconds and the server would be down for five minutes.

This status monitoring is per pair of servers. If one site has four RADIUS servers and their neighbour has three then that means twelve pairings. Thus only twelve failed responses in a five minute period could mean that the neighbour site is completely unavailable. Once a RADIUS server has marked all its neighbours as down and there's nowhere else to send auth requests it will respond to new auth requests with a Reject and continue to do so until there is a neighbour available.

Without this monitoring process RADIUS servers wouldn't know if they're sending auth requests towards systems that had truely failed and a proportion of attempts would simply disappear, leaving the user waiting.

This is why it is absolutely critical that all authentication attempts are responded to.

Every single one.

Where Jisc has a customer which is an individual member such failures as above only affect the users of that member. However, where the customer is a Federation the problem is much greater.

The Federation's RADIUS servers are likely doing exactly the above status monitoring of their members and marking their neighbouring RADIUS servers as zombies where appropriate.

Whilst this all might sound like everything is in hand, it's not.

If a request originates at a member, let's say camford.ac.uk, and is sent via Jisc to the Scarfolk Federation for the holby.nhs.uk site then it passes through a number of RADIUS servers on the way, each doing the same status checks on their neighbours.

So, let's say that the holby.nhs.uk decides not to respond to the requests. After 30s the Scarfolk Fed RADIUS servers will mark the first holby.nhs.uk RADIUS server as a zombie.

BUT, and here is the real problem, Jisc's NRPS don't see a response coming back from the Scarfolk Fed's server so Jisc will mark the first Fed server as a zombie. Even Camford might then mark the first Jisc RADIUS server as down.

A Federation will have multiple members and thus lots of traffic. More members means they're more likely to have a site failing to respond and thus appear to Jisc to be failing to respond. Federations are more likely to be marked as zombies.

So it's imperative that Federations do everything they can do ensure that their members respond to every requests.

Every single one.

We ask that members don't do this sort of status monitoring on neighbours 'above' them in their hierarchy. i.e. Camford and Scarfolk shouldn't apply it to Jisc, and Holby shouldn't apply to to Scarfolk's RADIUS servers. However, not all RADIUS servers are capable of this selective status checking.

The important message is that every RADIUS server should respond to every request, no matter what. No exceptions. No excuses.

From:
https://wiki.govroam.uk/dokuwiki/ - **Govroam**

Permanent link:
https://wiki.govroam.uk/dokuwiki/doku.php?id=public:frequently_asked_questions&rev=1743152878

Last update: **2025/03/28 09:07**