Aruba ClearPass Configuration for eduroam

Published 16/08/2022

Updated 14/03/2025

Configuring Aruba ClearPass for eduroam

- Aruba documentation
- Geant/UNINETT guide
- eduroam(UK) GUIDANCE

1) ARUBA Documentation

We do not have complete Jisc-produced documentation on configuring Aruba ClearPass for eduroam use, however the official Aruba ClearPass Deployment Guide may be useful together with the guide produced by UNINETT for Geant, which is good and contains eduroam-specific instructions. However the Geant guide contains some errors! You MUST read these in conjuntion with the Implementation roadmap [1].

Arbua ClearPass Policy Manager 6.10 Deployment Guide [2] : Aruba ClearPass Getting Started Guide [3]

Arbua ClearPass Policy Manager 6.9 Deployment Guide [4] : Aruba ClearPass Getting Started Guide [3]

2) GEANT Guide

>> Geant Guide to Configuring eduroam Using the Aruba Wireless Controller and ClearPass RADIUS [5] << **NOTE - this guide contains errors:**

i) ALERT Ref. Configuration of an 'Authentication Source' of the NRPSs to which eduroam visitors' authentication requests can be forwarded - this is NOT our preferred solution. See recommendations below in preference to step 6 in the above guide. Therefore you can **skip Step 1 of the Geant/UNINETT guide**.

ii) WARNING! Ref. Step 4 Configuration of service for handling authentications for own users on campus. Page 17, Step 4 - setting the conditions to filter authentication requests for own users on Wi-Fi service. The screenshot (Fig. 3.4) of the Service Rule shows the Condition: Service-Type must belong to Login-User (1), Framed-User (2) or Authenticate-Only (8). This is wrong because the value (1) Login indicates captive portal type authentication and the value indicates (8) Authenticate Only indicates MAC auth.

Service-Type is important, but it must be set to (2) Framed, i.e. Framed-User (2).

iii) WARNING! Ref. Step 5 Configuration of service for handling authentications received from the NRPS. Page 21, Step 5 - setting the conditions to identify authentication request types and determine how these types are to be handled (setting Network Policies/Authentication conditions) for your roaming users. The screenshot of the Service Rule shows the Condition: NAS-Port-Type must equal Wireless-802.11 (19). This is wrong and it is NOT necessary for authentication requests received from the NRPS. Do not include this condition.

NAS-Port-Type attribute is not guaranteed to be present in Access-Requests from roaming user authentications from remote Visited sites you have no control over. The only attributes that should be present ***if included by the Visited site*** are listed in section 2.1 of the Technical Specification.

3) eduroam(UK) GUIDANCE

3.1 Own users on campus - handling authentication requests (received from your campus service)

Follow Step 4 in the Geant–UNINETT guide [5] but be aware of errors in the Service Definition.

Creating an ‘eduroam-local Service’ comprises 4 elements:

1. a Service Rule
2. a set of conditions which must be met for the service rule to be effected
3. configuration of authentication including methods and authentication sources
4. configuration of VLAN assignment using Roles and Enforcement

i) Create an 802.1X Wireless Access Service

Navigate to Configuration > Services. Click on ‘Add’. On the Service tab, select ‘802.1X Wireless’ from the Type: drop down menu. The 802.1X Wireless service configuration dialog will open. You can enter a name for the service, e.g. eduroam-local

Configuration > Services > Add

ii) Specify the conditions you wish to be matched for the Service to be applied - do this in the Service Rule panel. Selection should be based on: network access medium = Wi-Fi; authentication service type = 802.1X; IP addresses of devices = local wireless LAN; and usernames = contains a userID component and your realm.

See p17 Fig 3.4 in the Geant–UNINETT guide

Service Rule: Matches ALL of the following conditions:

Type	Name	Operator	Value
RADIUS:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)

RADIUS:IETF	Service-Type	BELONGS_TO	Framed-User (2)
Authentication	Full-Username	MATCHES_REGEX	(?i).*@.*camford\.ac\.uk$ (*)
Connection	Src-IP-Address	BELONGS_TO_GROUP	Local controllers
and optionally:			
RADIUS:IETF	Called-Station-Id	CONTAINS	eduroam (**)

(*) **Full-username**: matching of your own users is needed for this Service. These are defined by having realm component equal to your own realm(s). You should only authenticate users utilising the correct realm; username which contain errors should be caught with a separate Service or not processed at all. (Nb. Users with errors in the username should however NOT be forwarded to the NPRS via the Service for your visitors (which matches on non-local realm name)).

/.*@.*camford\.ac\.uk$/i - this should match all userIDs@any_realm_ending_in_camford.ac.uk [6] (i.e. including subrealms) (case insensitive)

(?i).*@.*camford\.ac\.uk$ - is a tested case insensitive alternative

If your organisation uses **multiple realms** you can use the OR operator | e.g. (?i).*@.*(cam|camford|camfordshire)\.ac\.uk$

You could use quantifiers a capturing group () - if you use abbreviated forms of your realm - e.g. (?i).*@{1}.*cam(ford)?\.ac\.uk$ would match '@cam.ac.uk' and '@camford.ac.uk' The use of the {1} quantifier ensures that @ is only present once and the ? quantifier allows 'ford' to be present zero or only once. Although correct, these have not been tested with Clearpass.

It is recommended to not use the \b word boundary.

(**) Called-Station-Id: some APs append the SSID name to their MAC address in the Called-Station-Id attribute - this can be used to select auth requests arising from the eduroam SSID on your campus network and exclude requests arising from other SSIDs. Hint - You could create additional Services with relevant conditions to handle auth requests arising from other SSIDs configured on your network (e.g. govroam).

NAS-Port-Type: If you are only supporting Wi-Fi access with eduroam (as is most common), the value to use is ‘19’ i.e. Wireless-802.11.

Service-Type: this attribute indicates the type of service requested or the type of service to be provided. The most commonly used values are:

Value	Description	Operator
1	Login	Captive Portal

2	Framed	802.1X
3	Authenticate Only	MAC authentication

For eduroam, the value is ‘2’ i.e. Framed (2). (Framed-User).

Src-IP-Address: This is the NAS-IP-Address ie the IP addresses of your APs/WLC.

iii) Configuration of authentication including methods and authentication sources - follow the Geant–UNINETT guide [7]

iv) Configuration of VLAN assignment using Roles and Enforcement - follow the Geant–UNINETT guide [7]

3.2 Your roaming users authentication - RADIUS config and auth request handing (received from the NRPS)

Configuration > Services > Add (eduroam-inbound)

Addition of the NRPS to the RADIUS clients configuration of your Clearpass appliances and configuration of a Service to handle authentication requests received from the NRPS to support your roaming users.

i) Configuration > Network > Devices > Add. Enter the NRPS names, IP addresses, shared secrets. Use 'IETF' as Vendor Name. No not enable RADIUS CoA for the NRPS (only for your WLCs).

ii) Configuration > Network > Device Groups > Add. Create a group for the eduroam NRPSs (e.g. 'eduroam NRPSs') and add the NRPSs to the list of servers in the group.

iii) Configuration > Services > Add. Create a Service for your roaming users (e.g. Requests From NRPS). Click on Service tab and define the Conditions to be matched: a) Connection, ‘Src-IP-Address’ belongs to server group 'eduroam NRPSs' b) Authentication, 'Full-username' matches regex - see Geant Clearpass guide. You will also need to specify the authentication method you are supporting and the authentication source e.g. servername of your domain controller/LDAP database).

Conditions: For roaming user authentications **do NOT** define Conditions based on RADIUS attributes that are not guaranteed to be in the Access-Request from your roaming users at a Visited sites you have no control over! e.g. **Do NOT** specify NAS-Port-Type=wireless-802.11 (19). The only attributes that are guaranteed to be present are listed in section 2.1 of the Technical Specification.

3.3 Visitors - RADIUS config and auth request handling (forwarding of visitor auth requests to the NRPS)

Ref. Configuration of service to forward authentication requests from your eduroam SSID to the NRPS servers for your visitors: Configuration > Services Add (eduroam-outbound)

Page 22, Step 6 relates to configuring a Service with conditions that assume own-institution-users have been handled by an preceding service (eduroam-local) and that the only

conditions to be matched are that the requests come from the local WLAN (using NAS-IP-Address belongs to local controllers group) and the username must contain an '@'. The guide recommends that such requests are handled by the 'Authentication Source' which comprises the NRPS in primary and backup mode only. ***This approach is unsatisfactory.*** In addition the guide states that when creating the Service, the type 'RADIUS Enforcement (Generic)' should be selected, however we recommend that type 'RADIUS Proxy' is selected.

It is recommended to not use the Authentication sources method (which you would do via Configuration > Authentication > Sources) since this only allows for two remote RADIUS servers to be defined in the ‘eduroam NRPS’ Authentication Sources group - primary and backup.

Instead, the recommended method is to creating a ‘RADIUS Proxy Service’ with the NRPSs configured as ‘RADIUS Proxy Targets’. RADIUS Proxy Service configuration comprises six elements:

1. definition of Proxy Targets
2. a Service Rule
3. a set of conditions which must be met for the service rule to be effected
4. selection of the Proxy Targets to be employed
5. selected proxying scheme
6. ensure Accounting packets are not forwarded to the NRPS

i) **Proxy Targets** - Define each NRPS as a RADIUS Proxy Target - Navigate to Configuration > Network > Proxy Targets, then click on ‘Add’. The 'Add Proxy Target pop-out box will open. Enter the requisite informatation for each NRPS (select 'RADIUS' as the protocol option) and click [Save]. Do this for all three NPRS (roaming0.ja.net, roaming1.ja.net and roaming2.ja.net). (This is referred to as Step 2 in the geant guide).

ii) **Create a RADIUS Proxy Service** - Navigate to Configuration > Services, then click on 'Add'. On the 'Service' tab: Type - select 'RADIUS Proxy'. Name - enter a logical name (e.g. 'eduroam-outbound'/'proxy eduroam visitors to eduroam').

iii) **Conditions to be met for Service to be applied** - for forwarding auth requests to NRPS it is recommended that the eduroam-outbound service should be configured with authentication conditions that reduce the number of auth requests with 'bad usernames' being forwarded to the NRPS as per lines 1 and 2 of the following table.

Service Rule: Matches ALL of the following conditions:

Type	Name	Operator	Value
Authentication	Full-Username	MATCHES_REGEX	.*@[A-Za-z0-9-]+(\.[A-Za-z0-9-]+)*(\.[A-Za-z]{2,4})$

Authentication	Full-Username	NOT_CONTAINS	@'localrealm.', (*) 3gppnetwork, @gmail, @hotmail, @yahoo, @outlook, @live.co
Connection	Src-IP-Address	BELONGS_TO_GROUP	local WLC (**)
and optionally:			
RADIUS:IETF	Called-Station-Id	CONTAINS	eduroam (***)

(*) e.g. @camford., @student.camford., @staff.camford. ; ie @.*camford\.ac\.uk$ should work; to catch frequent misspellings of camford you would need to include the frequent mispelling explicitly.

(**) Whatever name you give to the group of your campus wireless LAN controllers/APs.

(***) Some APs append the SSID name to their MAC address in the Called-Station-Id attribute - this can be used to select auth requests arising from the eduroam SSID on your campus network and exclude requests arising from other SSIDs.

iv) **Specify Proxy Targets** - which remote RADIUS servers to forward authentication requests to. Click on the Proxy Targets tab. Proxy Targets - using the 'Select to Add' dropdown, add all three NRPSs as defined in the Proxy Targets definition step above.

v) **Proxying Scheme** - in the Proxy Targets tab, for the Proxying Scheme select (click on) the 'Load Balance' option rather than 'Failover'.

vi) **Accounting Requests**: Untick the ‘Enable proxy for accounting requests’ box

Nb. You can define the RADIUS attributes to be filtered out from Access-Challenge/Accept replies from the NRPS if you wish.

Click [Next]

Click the Enforcement tab

You can apply Enforcement parameters as required.

Click on the [Save] button

Ref: Aruba ClearPass Policy Manager - RADIUS Proxy Service [8]

3.4 Ordering the Services

Be sure that the services are listed in the following order:

- eduroam-local
- eduroam-inbound
- eduroam-outbound

With RADIUS systems auth requests are handled by the services in order until the request matches all the configured conditions - at which point the auth is processed by that service. If a complete match is not found the auth request is passed to the next service in the list.

3.5 Multiple ClearPass Server Deployments

As national RADIUS proxy operators we do not have direct experience in the deployment of multiple ClearPass servers and would welcome contributions from the community (e.g. in Deploying Policy Manager Clusters)

If you find any errors or omissions, wish to add content or have any comments on this page, please e-mail eduroamuk@jisc.ac.uk *[9]*

Links
[1] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-1
[2] https://www.arubanetworks.com/techdocs/ClearPass/6.10/PolicyManager/Content/Deploy/About%20ClearPass/Intro
[3] https://www.arubanetworks.com/techdocs/ClearPass/6.9/PolicyManager/Content/Get_Start_Guide/Hardware%20Ap
[4] https://www.arubanetworks.com/techdocs/ClearPass/6.9/Aruba_DeployGd_HTML/Content/About%20ClearPass/Intr
[5] https://archive.geant.org/projects/gn3/geant/services/cbp/Documents/cbp-79_guide_to_configuring_eduroam_using_the_aruba_wireless_controller_and_clearpass.pdf
[6] mailto:userIDs@any_realm_ending_in_camford.ac.uk
[7] http://Geant Guide to Configuring eduroam Using the Aruba Wireless Controller and ClearPass RADIUS
[8] https://www.arubanetworks.com/techdocs/ClearPass/6.10/PolicyManager/Content/CPPM_UserGuide/Services/Servi
[9] mailto:eduroamuk@jisc.ac.uk