GÉANT
Networks • Services • People

Guide to Configuring eduroam Using the Aruba Wireless Controller and ClearPass RADIUS

Best Practice Document

Produced by the UNINETT-led Campus Networking working group

Authors: Tom Myren (UNINETT), John-Egil Solberg (Intelecom)

April 2016

Document No: GN4-NA3-T2-UFS139
Version / date: V1.0 / 12.01.16
Original language : English
Original title: "Guide to Configuring eduroam Using the Aruba Wireless Controller and ClearPass RADIUS"
Original version / date: v1.0 / 12.01.16
Contact: campus@uninett.no

The work has been carried out by a UNINETT-led working group on campus infrastructure as part of a joint-venture project within the HE sector in Norway.

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 691567 (GN4-1).

Table of Contents

Table of Figures

Executive Summary

UFS 139 is a best practice document prepared by UNINETT in co-operation with Aruba, Intelecom Group AS and the HE sector's work group for mobility, gc-mobilitet@uninett.no.

This document describes one possible way of configuring eduroam on Aruba wireless controllers and utilizing Aruba ClearPass as a RADIUS server. Configuration of both wireless controller and the ClearPass Policy Manager is shown step-by-step using screenshots and some explanatory text.

The Technical Specification has received final approval after a four-week open consultation period with the HE sector.

1 Introduction

This document is a guide to configuring eduroam, including IEEE 802.1X, in an Aruba controller-based environment – i.e. a configuration based on one or more Aruba controllers that govern the traffic to and from local or remote Aruba access points. The guide applies to Aruba 600 Series, 3000 Series, 6000 and 7200 Series Mobility controllers all running the same ArubaOS (tm). All the configuration examples are from a 3600 controller (Refer to UFS 127 for Cisco controllers).

This best practice document specifically provides instructions and advice for configuration of Aruba equipment – that is wireless controllers and ClearPass RADIUS. For network planning, physical installation of access points, configuration of FreeRADIUS or Windows NPS and details on the operation of 802.1X, refer to UFS127, UFS112 and UFS140.

The document is divided into two parts; the first is about Aruba wireless controller configuration and the second is on the configuration of ClearPass RADIUS.

It is assumed that the initial configuration (addresses, VLAN's, DNS and so on) is already in place. If you need assistance for the initial setup, please refer to the Aruba configuration guides, Validated Reference Design (VRD) or other initial guides. You will find several examples by doing a simple search.

2 Aruba Controller Configuration

This chapter is a step by step guide for configuring eduroam on an Aruba controller. The recommendations are based on information from Aruba, UNINETT and experience from implementations at different institutions in the Norwegian HE sector.

The configuration can be done via CLI or GUI.

Using either method, the following steps are needed:

1. **Create RADIUS Server(s)**
   Configuration > Authentication > Servers > RADIUS Server > Add (a name for the new server must be typed in first)
2. **Create RADIUS Server Group**
   Configuration > Authentication > Servers > Server Group > Add
3. **Create 802.1x Group Auth. Profile**
   Configuration > Authentication > L2 Auth. > 802.1x Auth. > Add
4. **Create User Roles**
   Configuration > Access Control > User Roles > Add
5. **Create AAA Profile**
   Configuration > Authentication > AAA Profiles > Add
6. **Create SSID Profile**
   Configuration > All Profiles > Wireless LAN > SSID Profile > Add
7. **Create Virtual AP**
   Configuration > All Profiles > Wireless LAN > Virtual AP Profile > Add
   Select SSID and AAA Profiles created above

Sections 2.1 and 2.2 below show examples of the above steps using GUI and CLI respectively.

2.1 GUI Details

Step 1: Configuration > Authentication > Servers > RADIUS Server > Add (a name for the new server must be typed in first).

Here, “new-radius” is added. Click Apply (bottom right in the GUI). Repeat for a second server.

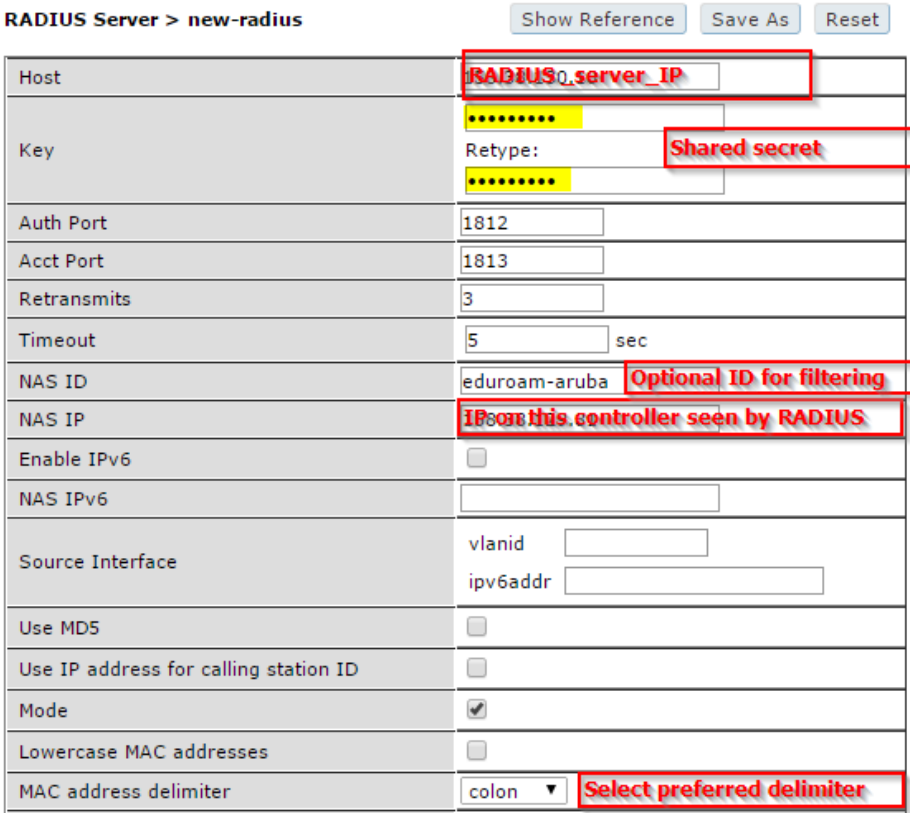


Figure 2.1: Adding a RADIUS server

Note: If you do not fill in the “NAS IP” above the IP entered under “Security > Authentication > Advanced || the Radius Client “NAS IPv4 Address” will be used as the source address. In a multi-controller environment, that field is by default copied from the Master Controller, meaning that authentication on a local controller will fail as the answer back from the RADIUS server will go to the Master. In other words, the “NAS IP” must be entered on local controllers.

Step 2: Configuration > Authentication > Servers > Server Group > Add (name of server typed first – here eduroam).

Add the above-defined servers to the Server Group (order defines priority).

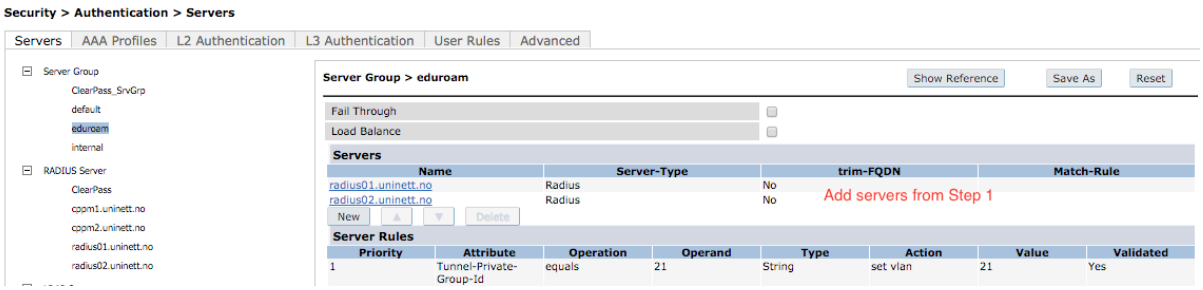


Figure 2.2: Adding a RADIUS server group

Note: It is possible (but not recommended) to use “Server Rules“ to set a User role or Vlan based on a wide range of conditions – for example a RADIUS parameter. Try adding a Server Rule to see all options.

Note 2: If you have an advanced RADIUS server (Freeradius, ClearPass etc.), it is better to place rules for Vlan or Role attributes on the RADIUS server, this makes both changes, documentation and troubleshooting easier.

Step 3: Configuration > Authentication > L2 Auth. > 802.1x Auth. > Add (type name of profile before add - here eduroam)

This is just to have a separate .1x profile to reference in the AAA profile.

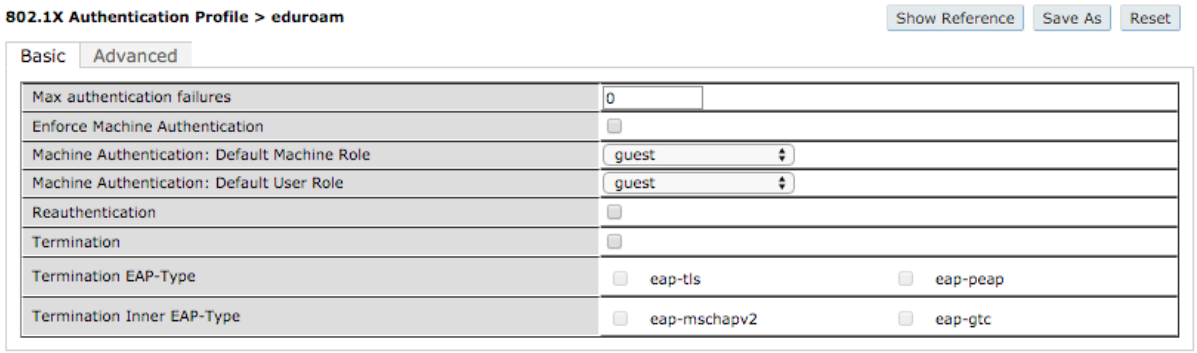


Figure 2.3: 802.1X authentication profile

Step 4: Configuration > Access Control > User Roles > Add (add new or edit existing)

You need to define two User Roles. One initial role (here, eduroam-logon) that block all traffic before successful authentication and a second role that is applied after authentication is completed. The Firewall policies defined under the “eduroam-authenticated” role should reflect your internal security policy (if not reflected elsewhere in your network configuration) and should also adhere to the eduroam policy (section 3.7 in Norwegian policy) stating which ports must be open as a minimum.

Figure 2.4: Defining User Roles

Step 5: Configuration > Authentication > AAA Profiles > Add (here, eduroam_AAA is added, then edit)

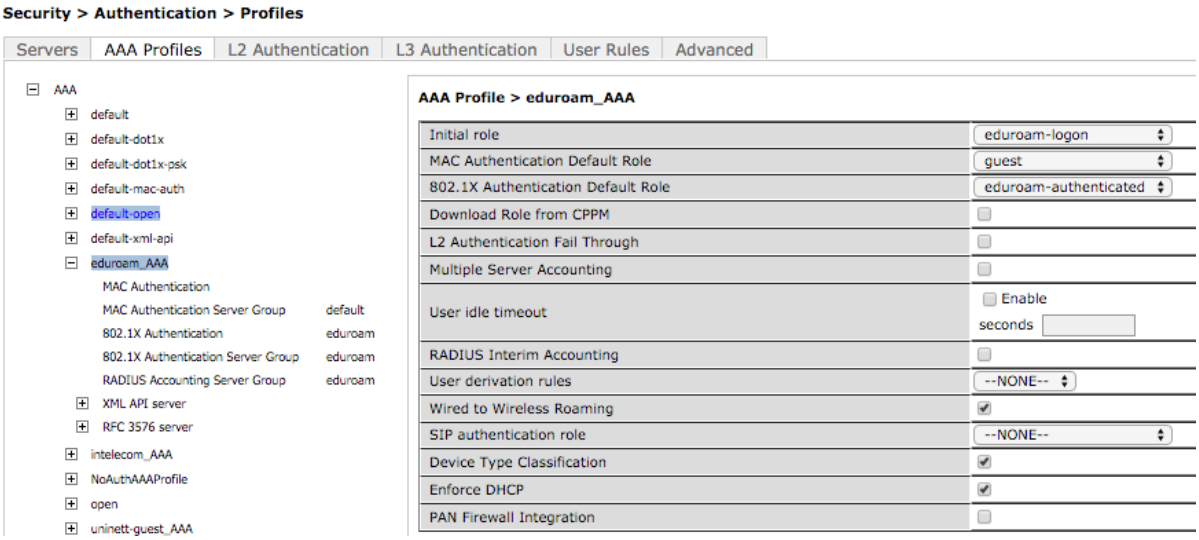


Figure 2.5: AAA profiles

Step 6: Configuration > All Profiles > Wireless LAN > SSID Profile > Add (the profile eduroam_SSID)

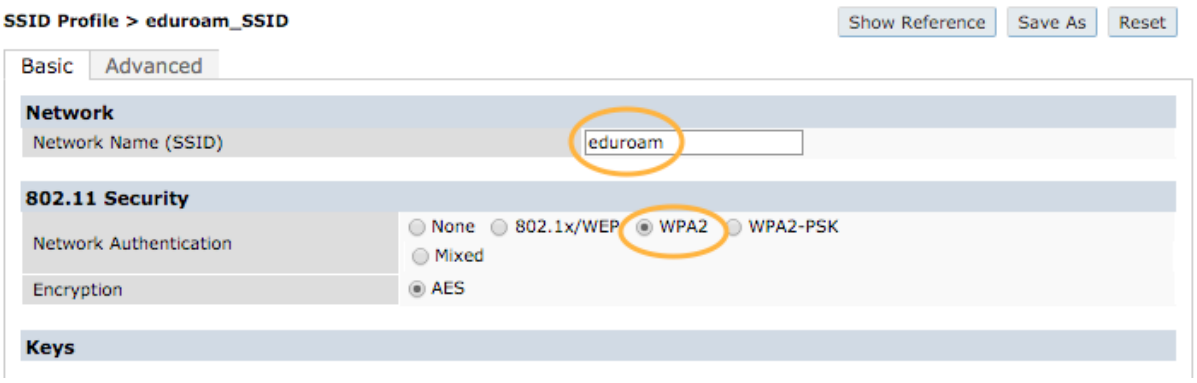


Figure 2.6: eduroam SSID profile

Under the Advanced tab, you might want to adjust the data rates offered on eduroam SSID. Note that all the 802.11b rates (1,2,5 and 11) as a minimum have been disabled in the example below.

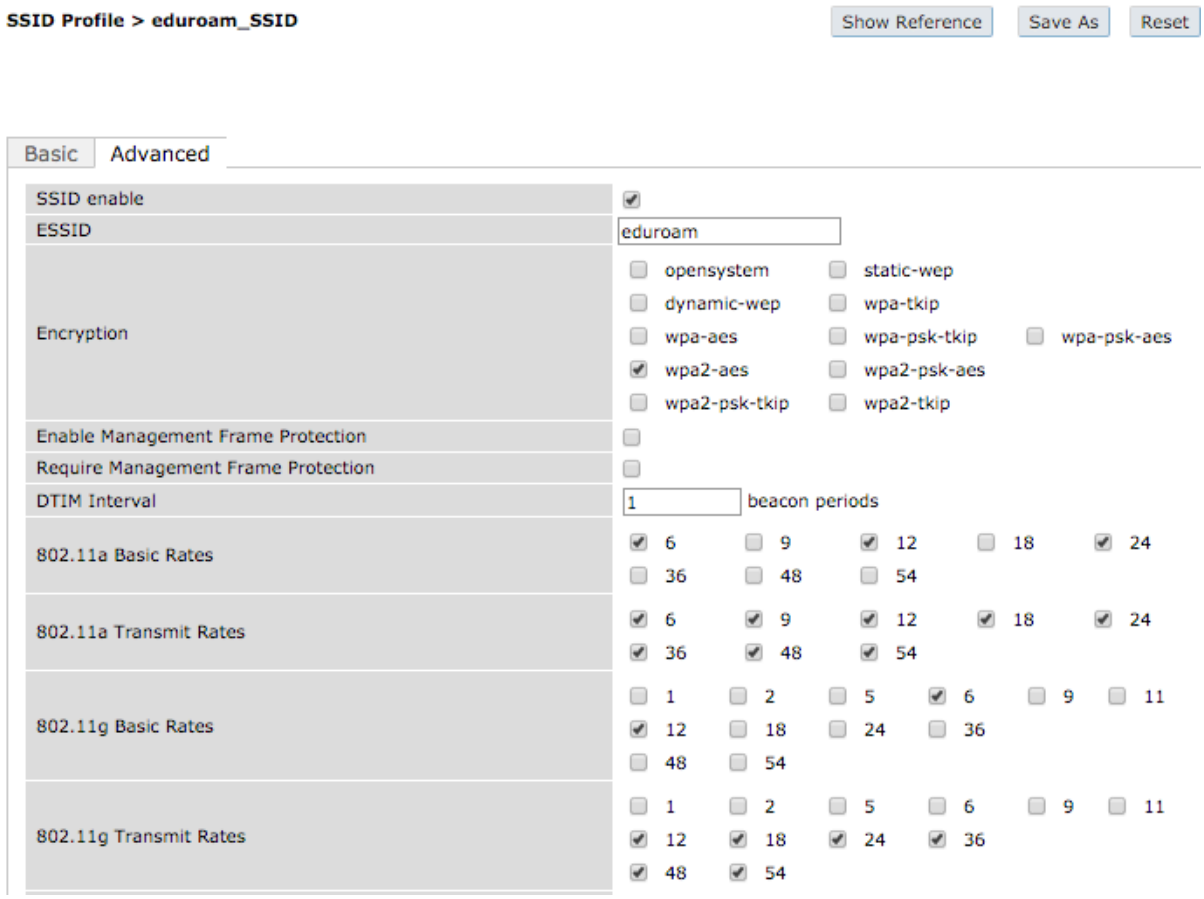


Figure 2.7: SSID profile advanced settings example

Step 7: Configuration > All Profiles > Wireless LAN > Virtual AP Profile > Add (here, eduroam_VAP)

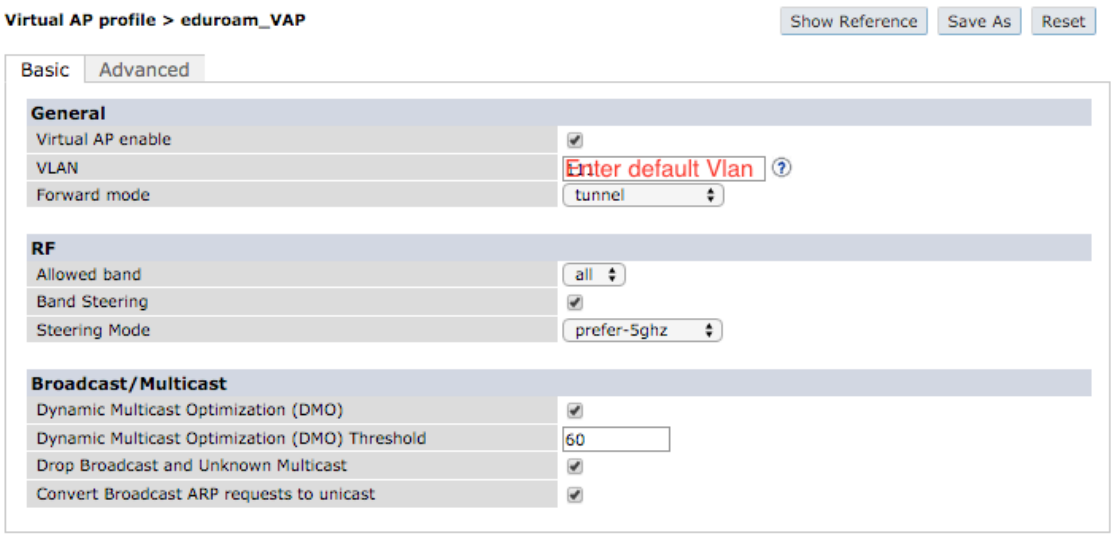


Figure 2.8: The Virtual AP profile

2.2 CLI Details

Below is a listing of CLI commands for the configuration that is described above using the GUI (you will find minor differences). Most of this can be used for cut and paste, but the x's must be replaced by your own data.

```
aaa authentication-server radius "radius01.xxxxxx.no"
  host "radius01.xxxxxx.no"
  key xxxxxxxxxxxxxxxxxxxxx
  timeout 20
  nas-identifier "xxxx_eduroam"
  nas-ip x.x.x.x
  mac-lowercase
  mac-delimiter colon
!
aaa authentication-server radius "radius02.xxxxxx.no"
  host "radius02.xxxxxx.no"
  key xxxxxxxxxxxxxxxxxxxxxxx
  timeout 20
  nas-identifier "xxxx_eduroam"
  nas-ip x.x.x.x
  mac-lowercase
  mac-delimiter colon
!
aaa server-group "eduroam"
 auth-server radius01.xxxxxx.no
 auth-server radius02.xxxxxx.no
! set vlan condition Tunnel-Private-Group-Id equals "xx" set-value "xx"
!
aaa authentication dot1x "eduroam"
  timer wpa-key-period 5000
!
ip access-list session block-all
  user any any  deny
  ipv6  user any any  deny
!
user-role eduroam-logon
 access-list session global-sacl
 access-list session apprf-eduroam-logon-sacl
 access-list session block-all
!
ip access-list session ra-guard
  ipv6  user any icmpv6 rtr-adv  deny
ip access-list session v6-allowall
  ipv6  any any any  permit
ip access-list session allowall
  any any any  permit
!
```

```
user-role eduroam-authenticated
 access-list session global-sacl
 access-list session apprf-eduroam-authenticated-sacl
 access-list session ra-guard
 access-list session allowall
 access-list session v6-allowall
!

aaa profile "eduroam_AAA"
  initial-role "eduroam-logon"
  authentication-dot1x "eduroam"
  dot1x-default-role "eduroam-authenticated"
  dot1x-server-group "eduroam"
  radius-accounting "eduroam"
  enforce-dhcp
!
wlan ssid-profile "eduroam_SSID"
  essid "eduroam"
  opmode wpa2-aes
!  g-basic-rates 6 12
!  g-tx-rates 12 18 24 36 48 54
!
wlan virtual-ap "eduroam_VAP"
  aaa-profile "eduroam_AAA"
  ssid-profile "eduroam_SSID"
  vlan  xxx
  band-steering
  dynamic-mcast-optimization
  dynamic-mcast-optimization-thresh 60
  broadcast-filter all
!
```

3 ClearPass RADIUS Configuration

This chapter describes how to implement eduroam using ClearPass as an AAA RADIUS server. The recommendations are based on information from Aruba, UNINETT and experience from implementations at different institutions in the Norwegian HE sector. The following guide assumes you already have a local authentication source defined on ClearPass and have a Radius server certificate in place. If this is not the case, please first refer to Appendix A for information on how to use Windows AD as an authentication source and Appendix B to install a server certificate on ClearPass. The local authentication source could be local user accounts or a connection to an LDAP server.

Before proceeding with the configuration, some planning and preparation is needed:

- If you are not already an eduroam Service Provider (SP) or Identity Provider (IdP), read the [Join] information on the Norwegian eduroam website. It describes what is required to become an SP or IdP in Norway. Alternatively, contact your NRO/NREN for details on how to become an eduroam provider.
- Verify which external IP-address(es) your ClearPass will use when communicating with the national proxy servers. Allow RADIUS AAA traffic to pass to this address, incoming with destination UDP 1812/1813 for IdP and answers with source UDP 1812/1813 for SP.
- Decide in which vlan and/or role you want to place eduroam users, and whether you want different vlan/roles for guests, students and staff. The recommendation is to use a guest vlan/role as default (configured on the controller) and have RADIUS (ClearPass) return a different vlan/role for students and staff when on their own premises. The vlan/role shall not be returned for own users while roaming.

The following steps are needed to setup ClearPass

1. Create Authentication sources (proxy targets) for the national servers (for SP)
2. Create Devices for all Wireless Controllers (SP and IdP) and national proxy servers (IdP)
3. Create Devices Groups for local controllers (SP and IdP) and national proxies (IdP)
4. Create “eduroam-local” service - local authentication, for local clients (IdP)
5. Create “eduroam-inbound” service - local authentication, for own roamers (IdP)
6. Create “eduroam-outbound” service for visitors (SP)

Section 3.1 below shows details of these 6 steps.

3.1 Configuration Details

Step 1: Configuration > Authentication > Sources – "Add"

Here you define the national proxies with shared secrets obtained from your NRO (National Roaming Operator). These sources (primary and backup) are used for proxy authentication requests from visiting eduroam users. We recommend using Authentication sources for this purpose to be able to set the Operator-Name attribute pre-proxy (this is not possible using "Proxy Targets" under Network).

Configuration » Authentication » Sources » Add - National proxies

Authentication Sources - National proxies

Summary | General | Primary | Attributes | Backup 1

General:

Name:	National proxies
Description:	Define national proxies as auth sources
Type:	RadiusServer
Use for Authorization:	Disabled
Authorization Sources:	-

Primary:

Server Name:	ntlr2.eduroam.no
Port:	1812
Secret:	********

Backup 1:

Server Name:	ntlr1.eduroam.no
Port:	1812
Secret:	********

Attributes:

RADIUS Pre Proxy Attributes:

	Type	Name		Value
1.	Radius:IETF	Operator-Name	=	1testing.no

RADIUS Post Proxy Attributes:

Figure 3.1: Defining national proxy targets

Note: Replace "1testing.no" with your realm "1<realm>.tld".

Step 2: Configuration > Network > Devices > Add

Here you define the clients that are allowed to send requests to this radius server. This is all national proxy servers and your own wireless controllers (or AP's). Enable RADIUS CoA (Change of Authority) for your own controllers but not for the national proxies. Allow the CoA port (default UDP 3799) to controllers. Set the correct Vendor Name for your controllers and use the IETF setting for national proxies. See example in following figure.

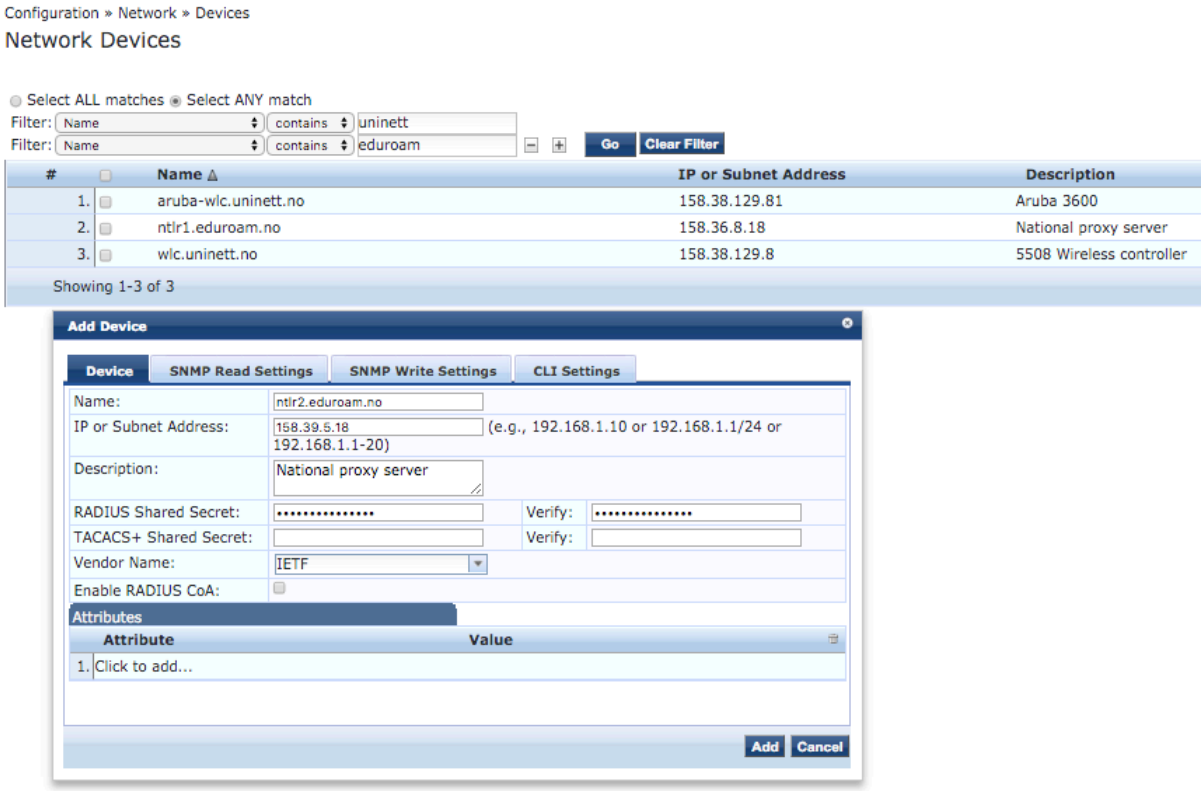


Figure 3.2: Defining network devices

Step 3: Configuration > Network > Device Groups > Add

Here you group the devices configured in Step 2 above into two device groups: national eduroam proxies and local controllers. This enables referencing in Services, which you will define in the next steps.

Figure 3.3: Defining network device groups

The local controllers device group should contain all your controllers defined in Step 2, and likewise all/both national proxies in the eduroam proxies group.

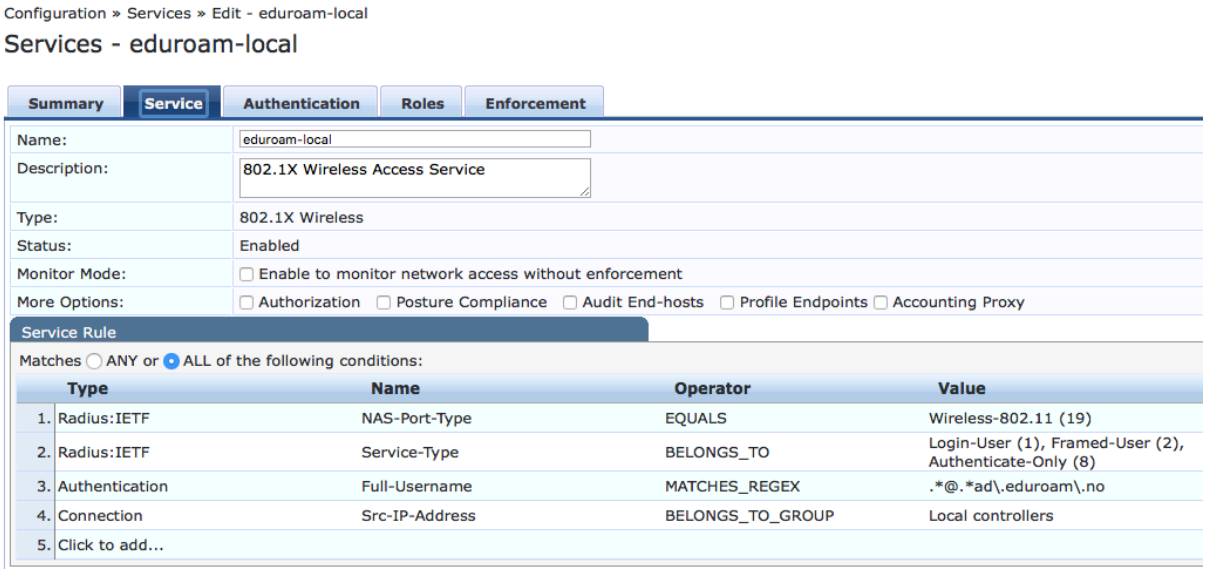
Step 4: Configuration > Services > Add (eduroam-local)

This service definition will authenticate local on-premises users. It is only needed if you are an IdP. This assumes you already have AD (or some other authentication source added to ClearPass), if this is not the case, please refer to Appendix A.

Eduroam users are by default placed in a VLAN as configured on your controller(s). It is in this service, under the "Enforcement" and "Roles" tabs, that you can change what local users are allowed to access by either placing them in a different vlan or assigning then to different roles.

Select type "802.1X Wireless" and enter the service name "eduroam-local" in the Service Tab.

Then "Click to add" service rules, so that you get:



Note: Regex for Full-Username here ".*@.*ad\.eduroam\.no$". Substitute ad.eduroam.no with your realm name.

Figure 3.4: Defining the eduroam-local service

In the Authentication Tab, select your AD as authentication source and the methods you support). See Appendix A for defining your AD as source. Below only PEAP is selected as an authentication method, some might choose EAP-TTLS (due to password format) or EAP-TLS for client certificate authentication.

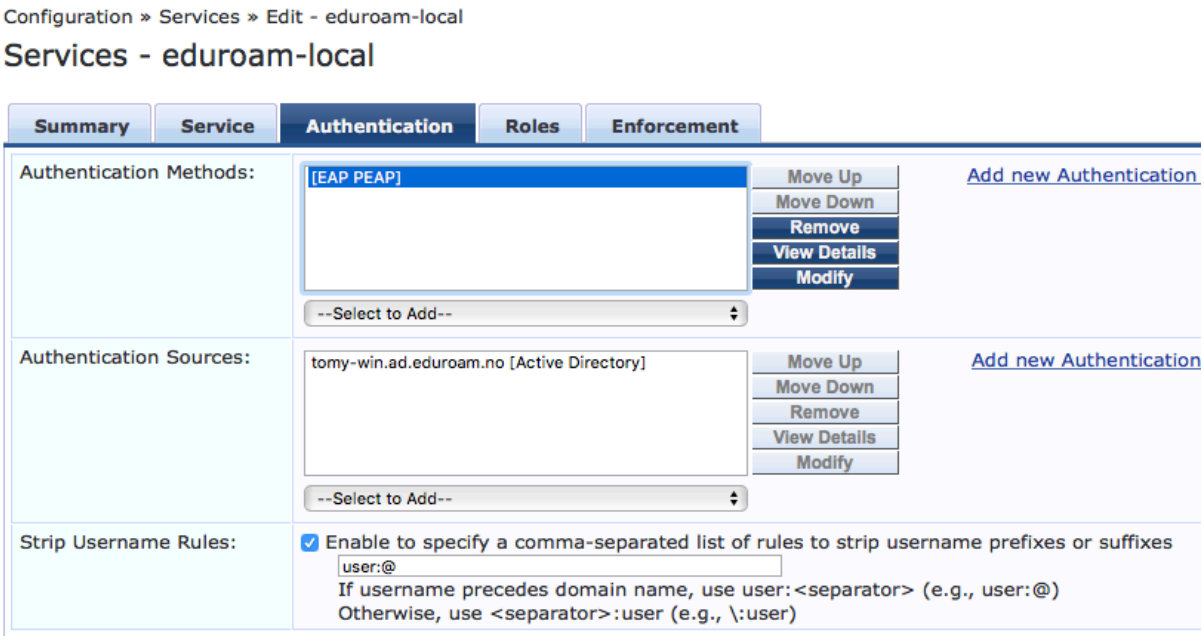


Figure 3.5 Add an authentication source to the eduroam-local service

Under the Roles Tab, you can assign roles that can be used in enforcement profiles to assign a vlan or other attributes to clients. There is a lot of flexibility in how this can be used.

The three figures below show how Group Membership in an AD is translated to a Role in ClearPass and that Role used to assign a VLAN through an Enforcement Profile. This is included as an example and is not the most practical solution, but does show the functionality. Examples of more straightforward methods to achieve similar results could be:

- Use the Aruba-User-Vlan attribute (instead of the Tunnel-Private-Group-ID), then an Aruba controller will accept the VLAN setting without additional configuration on the controller.
- Use Aruba-Named-Vlan attribute to set a VLAN pool that is defined on the controller. This will be beneficial for large user groups and / or fragmented ipv4 address ranges.
- Use Aruba-User-Role attribute to assign users into different “authenticated roles” on the controller and simply let all users use the default assigned VLAN pool from controller. I.e. let the controller define what the user is allowed and not the access-lists or firewall of the different subnets.

Configuration » Services » Edit - eduroam-local

Services - eduroam-local

Summary | Service | Authentication | Roles | Enforcement

Role Mapping Policy:	eduroam Modify

Role Mapping Policy Details

Description:	Convert AD group to Role
Default Role:	[Guest]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Role
1.	(Authorization:tomy-win.ad.eduroam.no:memberOf *CONTAINS* Ansatt)	[Employee]
2.	(Authorization:tomy-win.ad.eduroam.no:memberOf *CONTAINS* Norid)	[Contractor]

Figure 3.6 Example of using Roles in the eduroam-local service

Configuration » Services » Edit - eduroam-local

Services - eduroam-local

Summary | Service | Authentication | Roles | Enforcement

Use Cached Results:	☑ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	eduroam local authentication Policy Modify

Enforcement Policy Details

Description:	Setting Vlan using Enforcement Profiles
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* [Employee])	employee vlan enforcement
2.	(Tips:Role *EQUALS* [Contractor])	norid vlan enforcement
3.	(Tips:Role *EQUALS* [Guest])	[Allow Access Profile]

Figure 3.7 Example of using Enforcement in the eduroam-local service

Configuration » Enforcement » Profiles » Edit Enforcement Profile - employee vlan enforcement

Enforcement Profiles - employee vlan enforcement

Summary | Profile | Attributes

Profile:

Name:	employee vlan enforcement
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	1. Local controllers

Attributes:

	Type	Name		Value
1.	Radius:IETF	Termination-Action	=	RADIUS-Request (1)
2.	Radius:IETF	Tunnel-Type	=	VLAN (13)
3.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
4.	Radius:IETF	Tunnel-Private-Group-Id	=	21

Figure 3.8 Example enforcement profile referenced from Fig 3.7

Step 5: Configuration > Services > Add (eduroam-inbound)

This service will be triggered when own users connect to the eduroam service from other locations. You will use the same authentication source as the above service, but no roles/vlan/attributes are written back in the reply.

Configuration » Services » Edit - eduroam-inbound

Services - eduroam-inbound

Summary | Service | Authentication | Roles | Enforcement

Service:

Name:	eduroam-inbound
Description:	802.1X Wireless Access Service
Type:	802.1X Wireless
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Connection	Src-IP-Address	BELONGS_TO_GROUP	eduroam proxies
3.	Authentication	Full-Username	MATCHES_REGEX	.*@.*ad\.eduroam\.no

Authentication:

Authentication Methods:	EAP-PEAP eduroam
Authentication Sources:	tomy-win.ad.eduroam.no
Strip Username Rules:	user:@

Roles:

Role Mapping Policy:	-

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	[Sample Allow Access Policy]

Figure 3.9 The eduroam-inbound service

Step 6: Configuration > Services > Add (eduroam-outbound)

Create a new service of the type “RADIUS Enforcement (Generic)” to allow eduroam visitors to logon to your eduroam SSID, authenticating at their own institution.

In the following example, the Roles and Enforcement tabs are left unchanged, this can be adjusted according to your local preferences. The service is triggered by a username containing @ coming from a local controller, which means that is has to be ordered below the eduroam-local service.

Configuration » Services » Edit - eduroam-outbound

Services - eduroam-outbound

Summary | Service | Authentication | Roles | Enforcement

Service:

Name:	eduroam-outbound
Description:	Adding Operator Name attribute pre-proxy
Type:	RADIUS Enforcement (Generic)
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Authentication	Full-Username	CONTAINS	@
2.	Radius:IETF	NAS-IP-Address	BELONGS_TO_GROUP	Local controllers

Authentication:

Authentication Methods:	[EAP PEAP]
Authentication Sources:	National proxies
Strip Username Rules:	-

Roles:

Role Mapping Policy:	[Guest Roles]

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	[Sample Allow Access Policy]

Figure 3.10 The eduroam-outbound service

Note: In the example above, the Roles and Enforcement tabs are left with the default values. Enforcement could be used to overwrite any Vlan attributes contained in a reply from the remote Radius server. The reply should not contain such attributes, i.e. this would be an extra precaution. In such an Enforcement profile, you would need to overwrite your default Vlan for eduroam visitors.

Finally check that the defined Services are ordered correctly, as seen in following figure:

Configuration » Services

Services

Add
Import
Export All

Filter: Name contains Go Clear Filter Show 10 records

#	Order	Name	Type	Template	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	
2.	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	
3.	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	
4.	4	[Guest Operator Logins]	Application	Aruba Application Authentication	
5.	5	eduroam-local	RADIUS	802.1X Wireless	
6.	6	eduroam-inbound	RADIUS	802.1X Wireless	
7.	7	eduroam-outbound	RADIUS	RADIUS Enforcement (Generic)	

Figure 3.11 Defined services in the correct order

4 Conclusions

Combining Aruba wireless controllers and the ClearPass Policy Manager as a RADIUS server to provide the eduroam service is a fairly easy. ClearPass can also be used as a RADIUS in combination with controllers from other wireless product vendors. You get the same functionality (if not more) using a FreeRADIUS server.

The strengths of ClearPass are the user-friendly interface for configuration, monitoring and troubleshooting, combined with the ability to differentiate access based on client type and integration with Windows AD for authentication and authorization.

The drawbacks of course are that it is not freeware and, for some, the missing / limited CLI interface.

Appendix A Active Directory Integration

This appendix describes how to configure ClearPass to use Microsoft Active Directory as an authentication source. First, ClearPass must join the AD domain, then the authentication source can be added.

A.1 Joining ClearPass to an AD Domain

Joining AD is a simple operation, but before proceeding please note the following:

- Joining AD is only needed when performing EAP-PEAP authentication (so needed for eduroam)
- Ensure NTP synchronization is enabled on all servers
- The Active Directory account used by ClearPass to join the domain requires privileges to add computers to the domain, the account is not stored by CP and can be disabled or even deleted once the join operation is completed.
- Configure ClearPass to send DNS requests to the AD server
- Use the fully qualified domain name of the AD domain controller during join (just the domain name or IP might fail)
- When entering the username (if different from Administrator), use the format: username@domain
- Avoid using a dash (-) in the NetBIOS Name. It has been seen to cause AD join failure.

To join AD via GUI:

Go to: Administration > Server Manager > Server Configuration > Click the server, then “Join AD Domain”

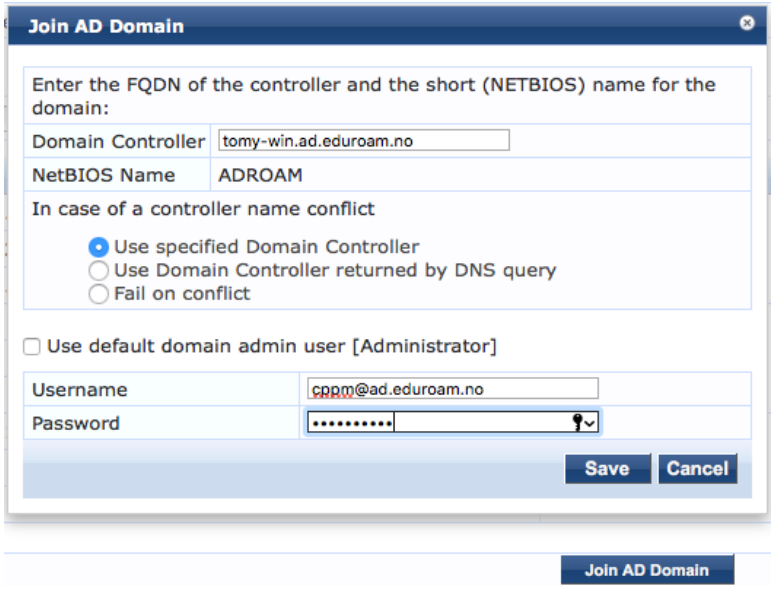


Figure A.1: Joining AD example

Alternatively, via CLI and the “appadmin” user, using “ad testjoin” to check or “ad netjoin”.

[appadmin@cppm-eval]# ad testjoin ADROAM

Join is OK

netjoin <domain-controller.domain-name> [domain NETBIOS name] [domain REALM name] [ou=<object container>]

A.2 Add AD as an Authentication Source

In CP; Configuration > Authentication > Sources > Add, then fill in according to the following figures.

Use a secure connection when possible.

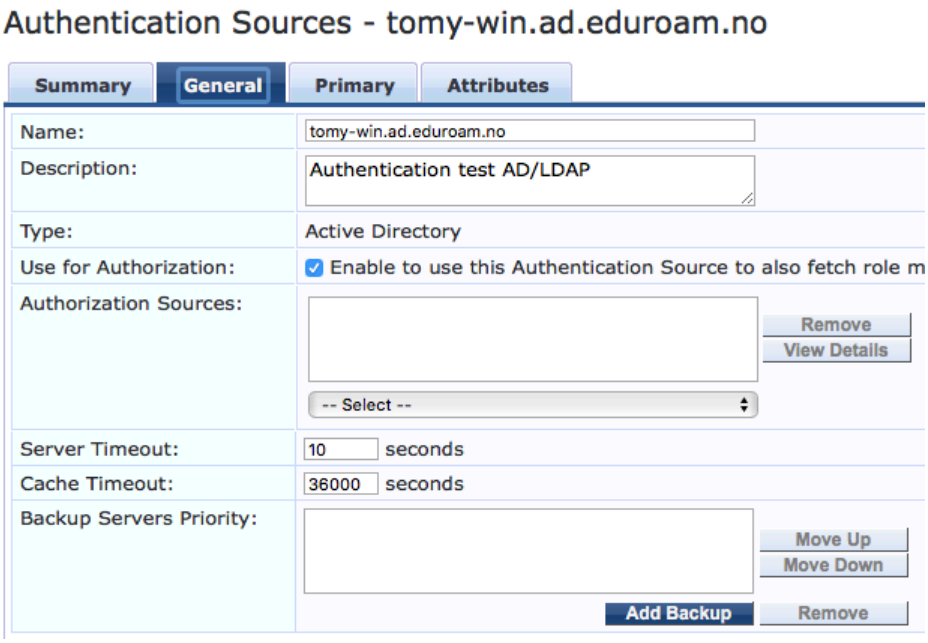


Figure A.2: Adding a source – general parameters

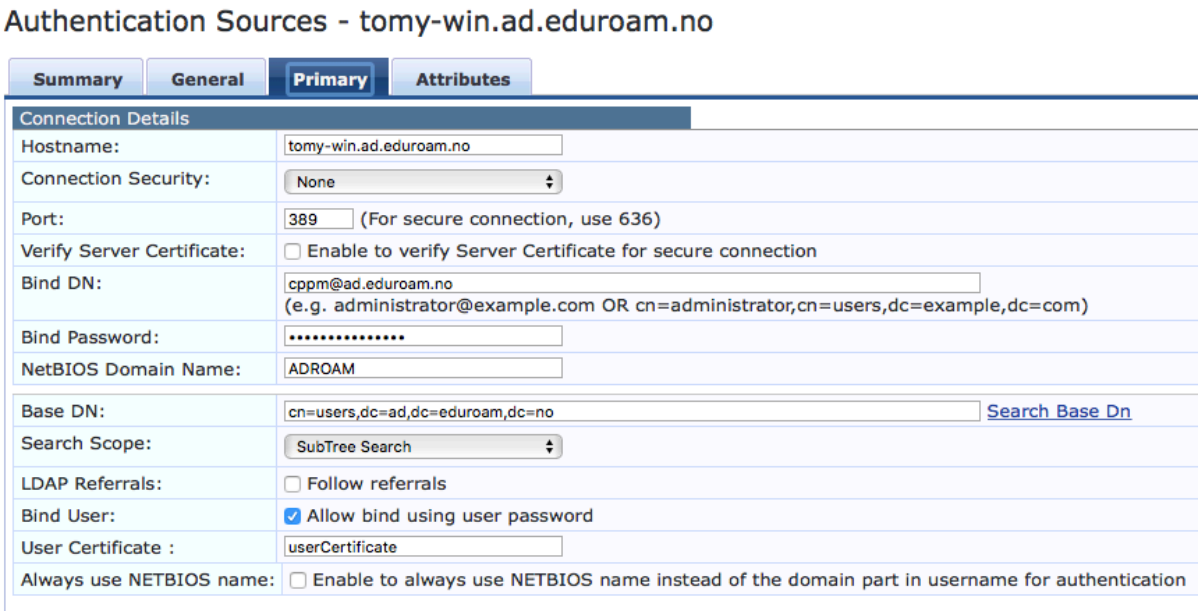


Figure A.3: Adding a source - Primary Tab

Appendix B Radius (ClearPass) Server Certificate

The Radius server needs a certificate (to establish a secure connection and for clients to verify the correct home server). This certificate can be issued by a local (own) CA, through Geant or any commercial CA, as for any eduroam installation. For eduroam certificate considerations, please see "EAP Server Certificate Considerations" on the GEANT Wiki pages [EAP].

ClearPass have the option of separate certificates for the https server and the radius server, so having a self-signed Radius certificate is an option (the https certificate must of course be from a well-known CA to work effectively).

Go to Administration > Certificates > Server Certificate, Select Type (Radius Server Certificate) and choose from the top left options.

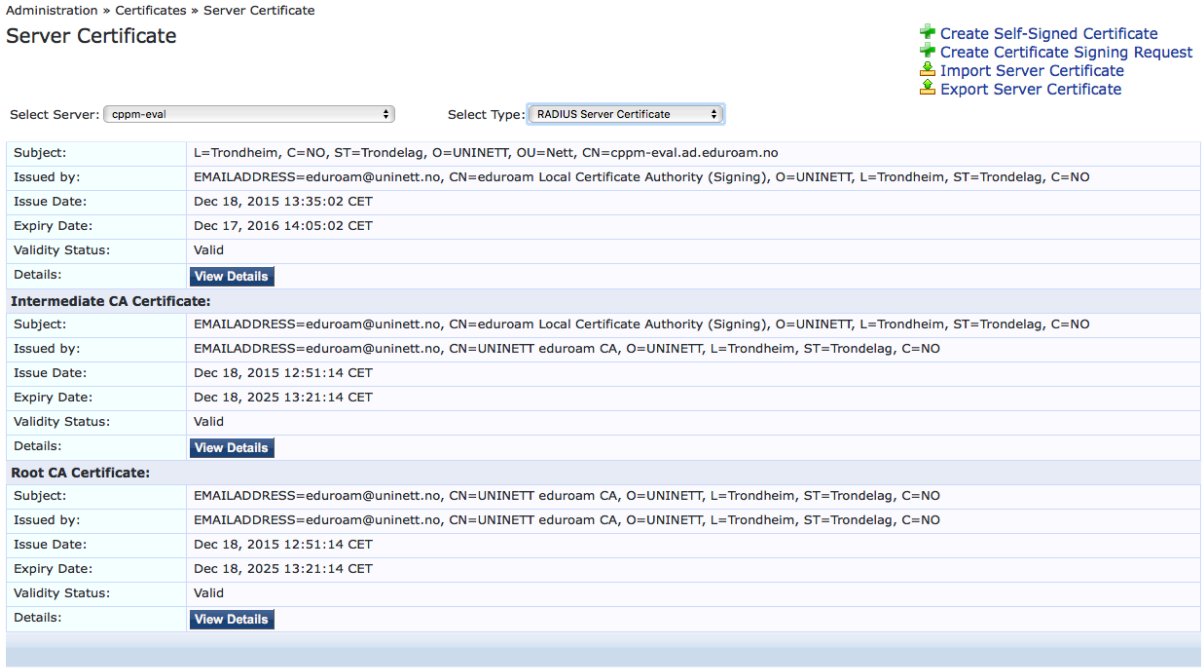


Figure B.1: Example of Self-signed Certificate

You can "Create Self-Signed Certificate", or "Create Certificate Signing Request" – send it to your preferred CA and then "Import Server Certificate" when the certificate comes back. Creating a Certificate Signing Request will prompt you for the necessary input (see the following figure) and produce a private key and CSR. You will need the private key file and password when eventually importing the certificate into ClearPass. It is therefore important to choose "Download" to have the private key when later installing the certificate (you will not be able to get it later without a new CSR).

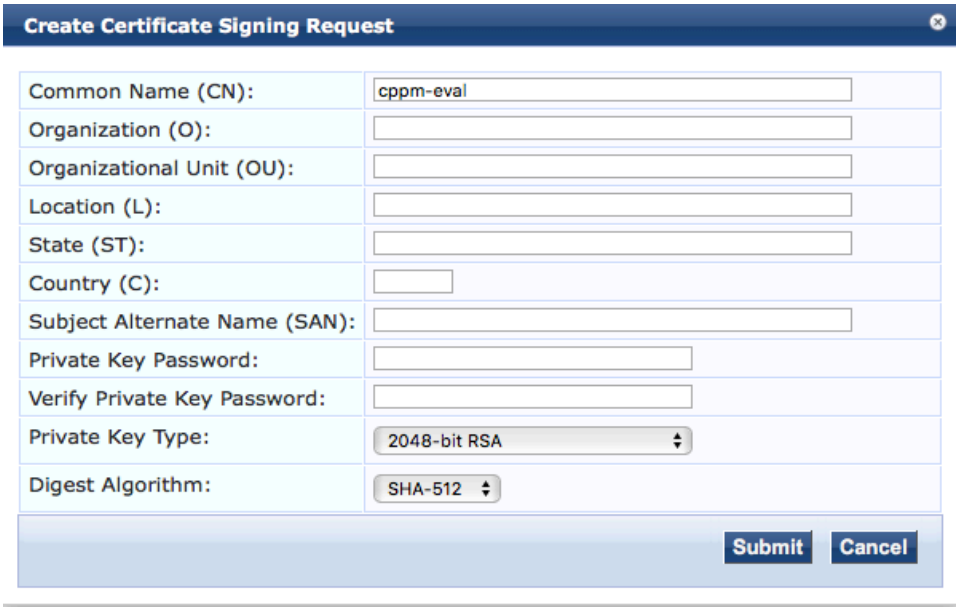


Figure B.2: Creating a Certificate Signing Request

Before importing the final server certificate received from your chosen CA, you need to import (and enable) the Root and Intermediate CA's under Administration > Certificates > Trust List.

Whatever certificate (private or public) you choose, you will need at least the CA certificate (many operators also include intermediates) to configure the eduroam clients. The recommended way is to use CAT (eduroam's Configuration Assistant Tool) to distribute the correct settings including the CA certificate to all the clients at your institution. For more information on setting up eduroam client profiles, please see "A Guide to eduroam CAT for Institution Administrators" [CAT].

References

[EAP] The GEANT wiki space on choosing the best suited EAP server
https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations

[CAT] The GEANT wiki space explaining the Configuration Assistant Tool administration interface
https://wiki.geant.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+institution+administrators

[Join] How to become an eduroam service or identity provider
https://eduroam.no/join

UNINETT best practice documents are available from https://www.uninett.no/ufs. Three of these are referenced in this document.

[UFS112] Recommended Security Systems for Wireless Networks

[UFS127] Guide to Configuring eduroam using a Cisco Wireless Controller

[UFS140] Using Windows NPS as RADIUS in eduroam

Glossary

802.1X	IEEE standard for port-based network access control
AAA	Authentication, Authorisation and Accounting
AD	Active Directory (Microsoft developed directory service)
BPD	Best Practice Document
CLI	Command Level Interface
CA	Certificate Authority
DNS	Domain Name Server
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol – Transport Layer Security
eduroam	EDUcation ROAMing
ETLR	European Top-Level RADIUS
FLR	Federation-Level RADIUS
GUI	Graphical User Interface
HE	Higher Education
IdP	Identity Provider
IEEE	Institute of Electrical and Electronics Engineers
NREN	National Research and Educational Network
NRO	National Roaming Operator
NTLR	National Top-Level RADIUS
PEAP	Protected Extensible Authentication Protocol
RADIUS	Remote Access Dial-In User Service
SP	Service Provider
SSID	Service Set Identifier
TLD	Top Level Domain
VLAN	Virtual Local Area Network
VRD	Validated Reference Design (Aruba best practices)
UFS	UNINETT FagSpesifikasjoner (Norwegian BPD)