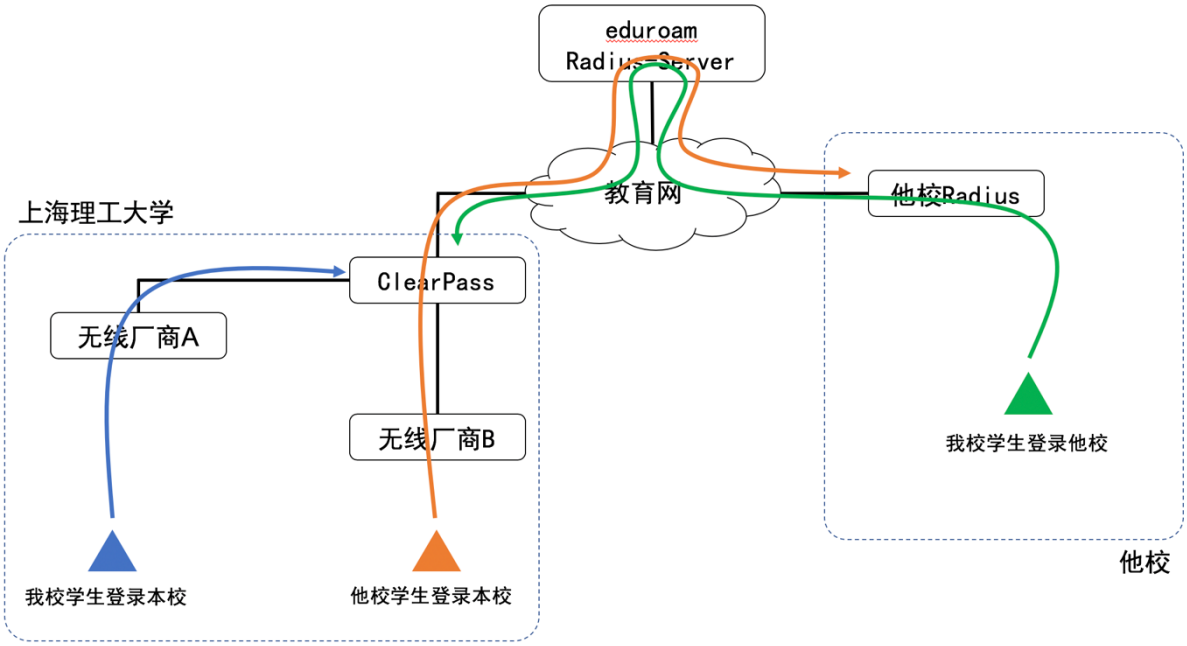
Table of Contents

越来越多的学校加入 eduroam，提供便利的同时更要保障安全性。本文以上海理工大学为例，展示了如何通过 ClearPass 成功实现在 eduroam 区分校内与校外用户的案例。

我校于 2017 年准备上线 eduroam 服务，此前学校无线主要认证方式为 Portal 认证，通过 eduroam，进一步促进学校无线从 Portal 认证向 802.1x 认证演进。

ClearPass 能够直接对接 eduroam Radius-Server，并且支持多个厂商，因此我校选择使用它来实现 eduroam。

eduroam 功能实现流程图如下：

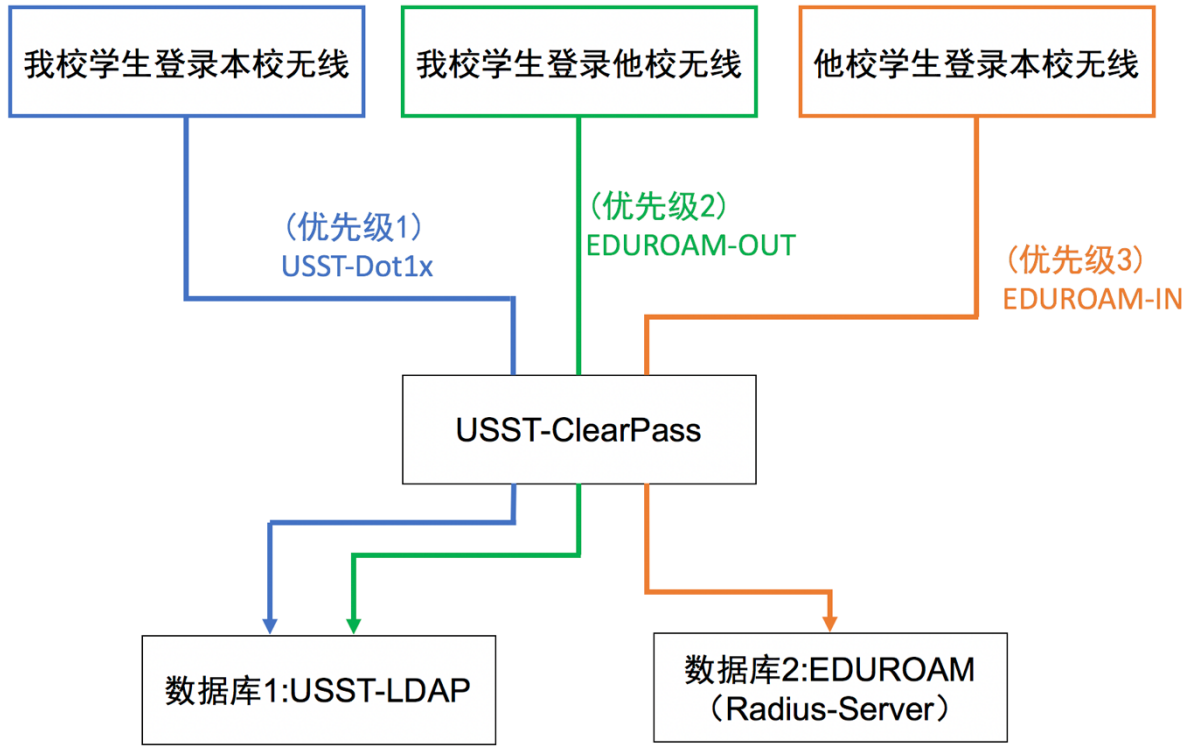


1. 区分校内与校外用户的三种认证入口

为了实现统一认证接口，ClearPass 认证服务器解决以下三种认证情况的认证需求：

- 我校学生登录本校无线
- 我校学生登录他校无线
- 他校学生登录本校无线

三种认证场景对应了三个 ClearPass 认证入口，如下：



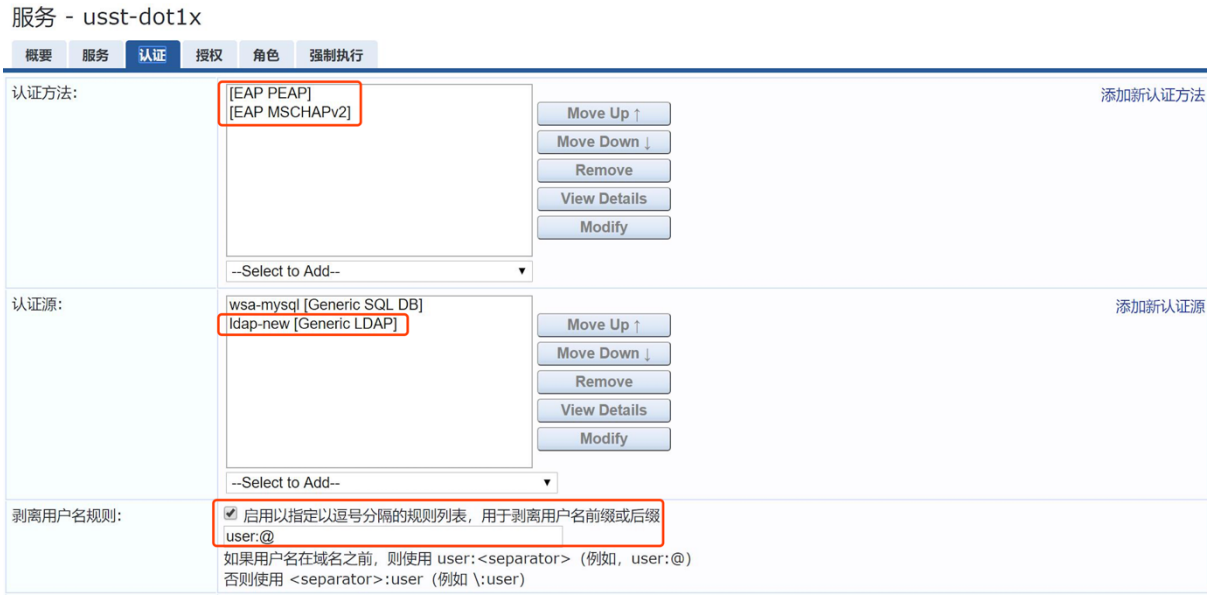
1.1 我校学生登录本校无线（USST-Dot1x）

1.1.1 认证入口匹配条件

- 用户名中包含@usst.edu.cn 则被认为是本校用户，对于同时拥有多个域名的学校，可以使用正则表达式来确定是否为本校用户。

1.1.2 认证入口认证方式以及数据源

- 认证方式：EAP-PEAP、EAP-MSCHAPv2
- 认证源：USST-LDAP
- 用户名规则：数据库中用户名不带@usst.edu.cn，因此需要提前剥除，格式为”user:@”，如要剥除前缀如 USST\user，则格式为”\:user”



1.1.3 权限策略

- 在 Clearpass 中特别标识 VIP 的用户，同时在线设备小于 10 台的情况下，分配 VIP 权限。
- 在 LDAP 数据库中，用户组为教师，同时在线设备小于 10 台的情况下，分配教师权限。
- 在 LDAP 数据库中，用户组为学生，同时在线设备小于 10 台的情况下，分配学生权限。
- 在 LDAP 数据库中，用户组非教师和学生，同时在线设备小于 10 台的情况下，分配默认权限。

- 在 LDAP 数据库中读不出用户组的情况下，拒绝登录。

服务 - usst-dot1x

概要 | 服务 | 认证 | 授权 | 角色 | 强制执行

使用缓存的结果:	使用从上一会话中缓存的角色和安全状况属性
强制执行策略:	usst-dot1x ▾ Modify 添加新强制执行策略

强制执行策略详细信息

说明:	
默认配置文件:	[Deny Access Profile]
规则评估算法:	first-applicable

	条件	强制执行配置文件
1.	(Tips:Role *EQUALS* usst-vip) *AND* (Authorization:[Insight Repository]:active_sessions_dot1x *LESS_THAN* 10)	usst-vip role
2.	(Tips:Role *EQUALS* usst-teacher) *AND* (Authorization:[Insight Repository]:active_sessions_dot1x *LESS_THAN* 10)	usst-teacher role
3.	(Tips:Role *EQUALS* usst-student) *AND* (Authorization:[Insight Repository]:active_sessions_dot1x *LESS_THAN* 10)	usst-student role
4.	(Tips:Role *EQUALS* usst-other) *AND* (Authorization:[Insight Repository]:active_sessions_dot1x *LESS_THAN* 10)	usst-other role
5.	(Authentication:Status *EQUALS* User)	[Deny Access Profile]

1.1.4 我校学生登录本校无线认证记录

请求详细信息

概要 | 输入 | 输出 | 警报

用户名:	171310063@usst.edu.cn
终端主机标识符:	8C34FD1ED3C6 (SmartDevice / Android / Android)
访问设备 IP/端口:	[redacted]

RADIUS 请求

Radius:Aruba:Aruba-AP-Group	ap-group-usst-classroom
Radius:Aruba:Aruba-Device-Type	Linux
Radius:Aruba:Aruba-Essid-Name	eduroam
Radius:Aruba:Aruba-Location-Id	sijiao-210
Radius:IETF:Called-Station-Id	001A1E045B30
Radius:IETF:Calling-Station-Id	8C34FD1ED3C6
Radius:IETF:Framed-MTU	1100
Radius:IETF:NAS-Identifier	edu-dot1x
Radius:IETF:NAS-IP-Address	[redacted]
Radius:IETF:NAS-Port	0

◀◀ ◀ Showing 2 of 1-601 records ▶ ▶▶ 更改状态 Show Configuration 导出 显示日志 关闭

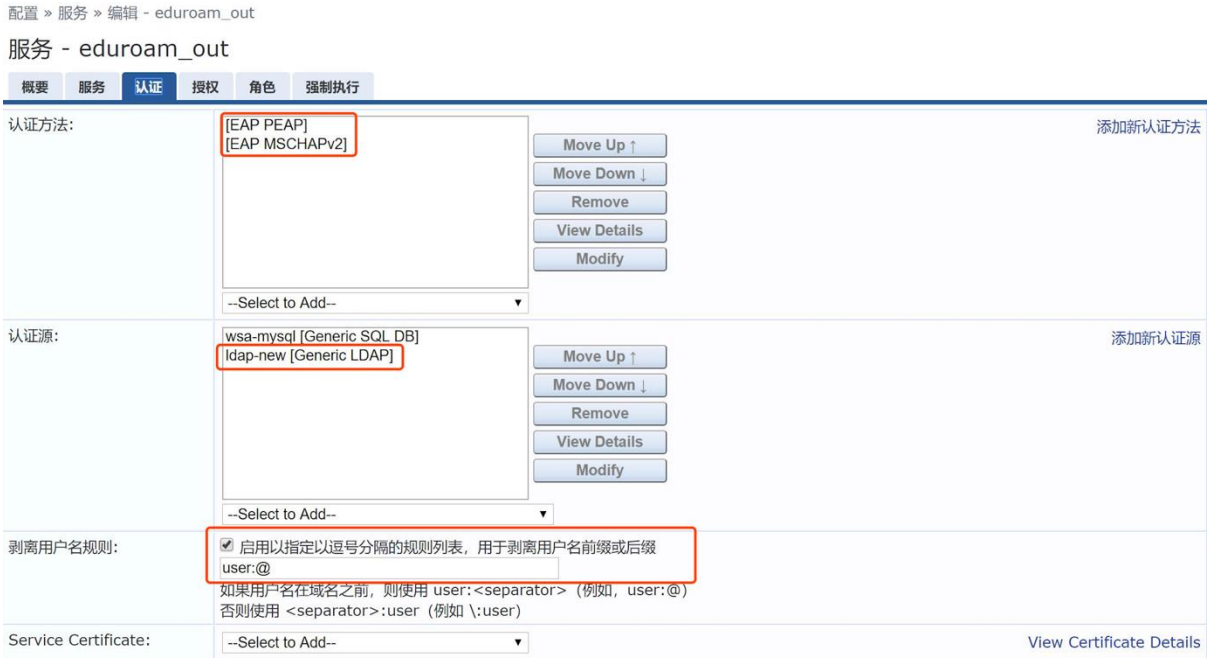
1.2 我校学生登录他校无线（eduroam-OUT）

1.2.1 认证入口匹配条件

- 认证源 IP 为 ilr1.edu.cn（162.105.129.2）以及 ilr2.edu.cn（162.105.129.5）则被认为是他校转发来的认证请求。

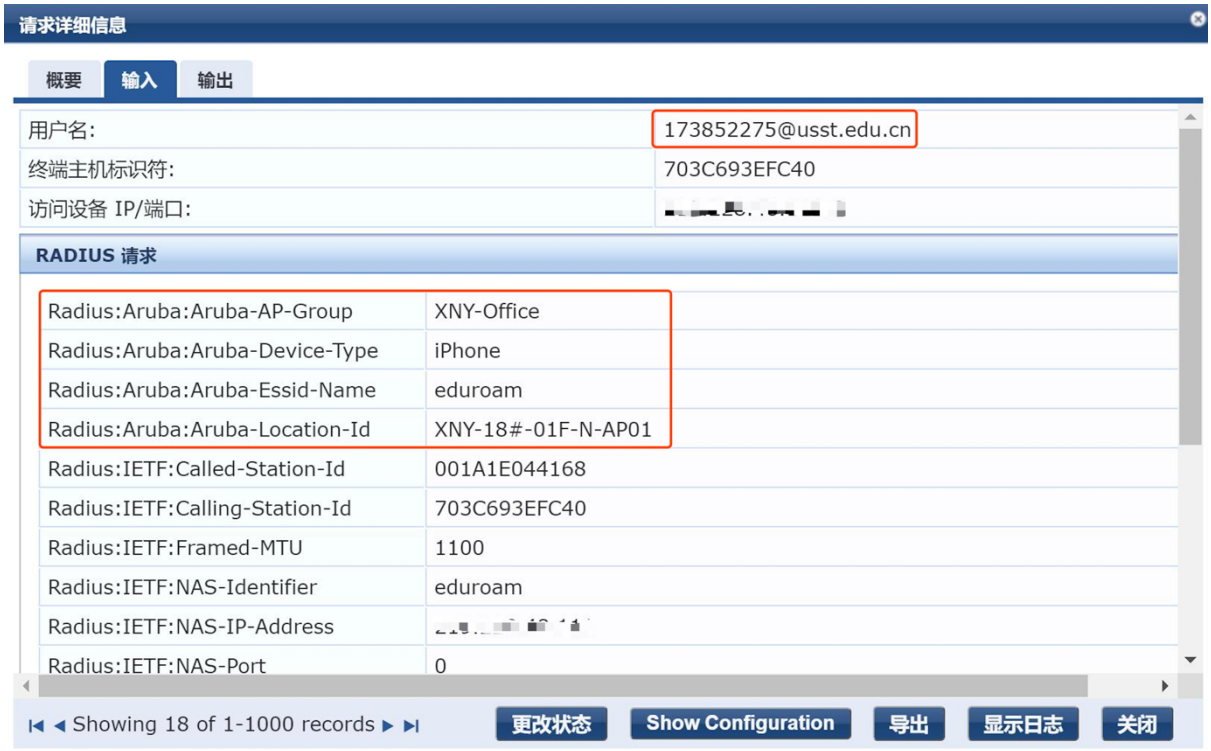
1.2.2 认证入口认证方式以及数据源

- 认证方式：EAP-PEAP、EAP-MSCHAPv2
- 认证源：USST-LDAP
- 用户名规则：数据库中用户名不带@usst.edu.cn，因此需要提前剥除，格式为”user:@”，如要剥除前缀如 USST\user，则格式为”\:user”



1.2.3 我校学生登录他校无线认证记录

以下为我校学生从上海健康医学院登录时的认证记录



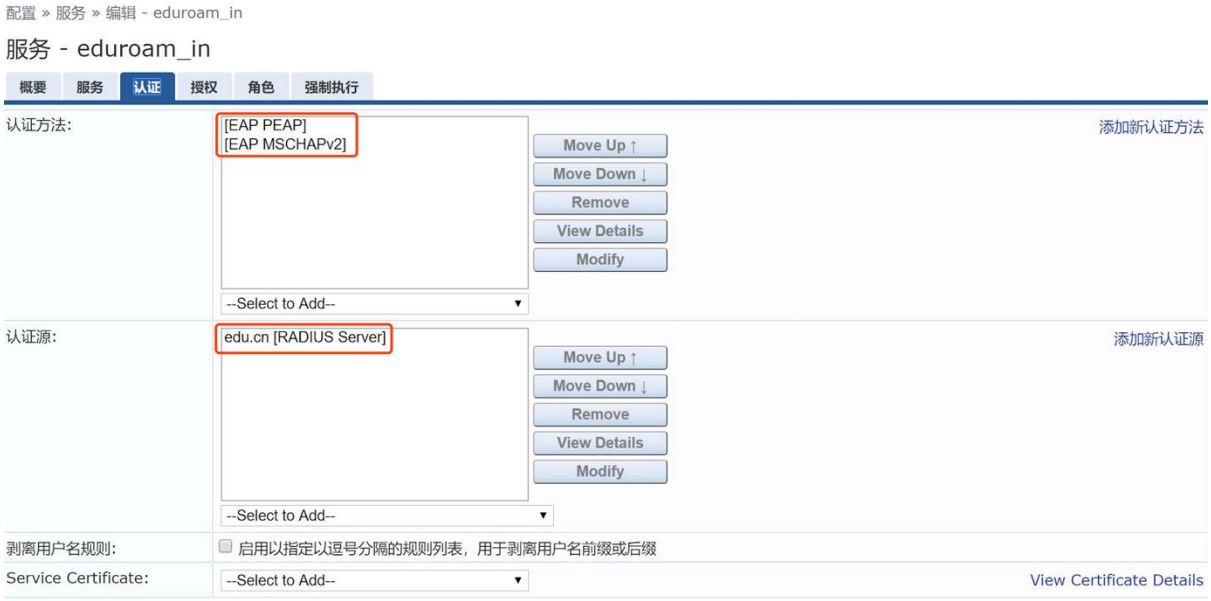
1.3 他校学生登录本校无线（eduroam-IN）

1.3.1 认证入口匹配条件

- 除了@usst.edu.cn 以外的后缀域名登录 eduroam，则被认为是他校学生在本校登录

1.3.2 认证入口认证方式以及数据源

- 认证方式：EAP-PEAP、EAP-MSCHAPv2
- 认证源：eduroam（162.105.129.2/162.105.129.5, Radius-Server）

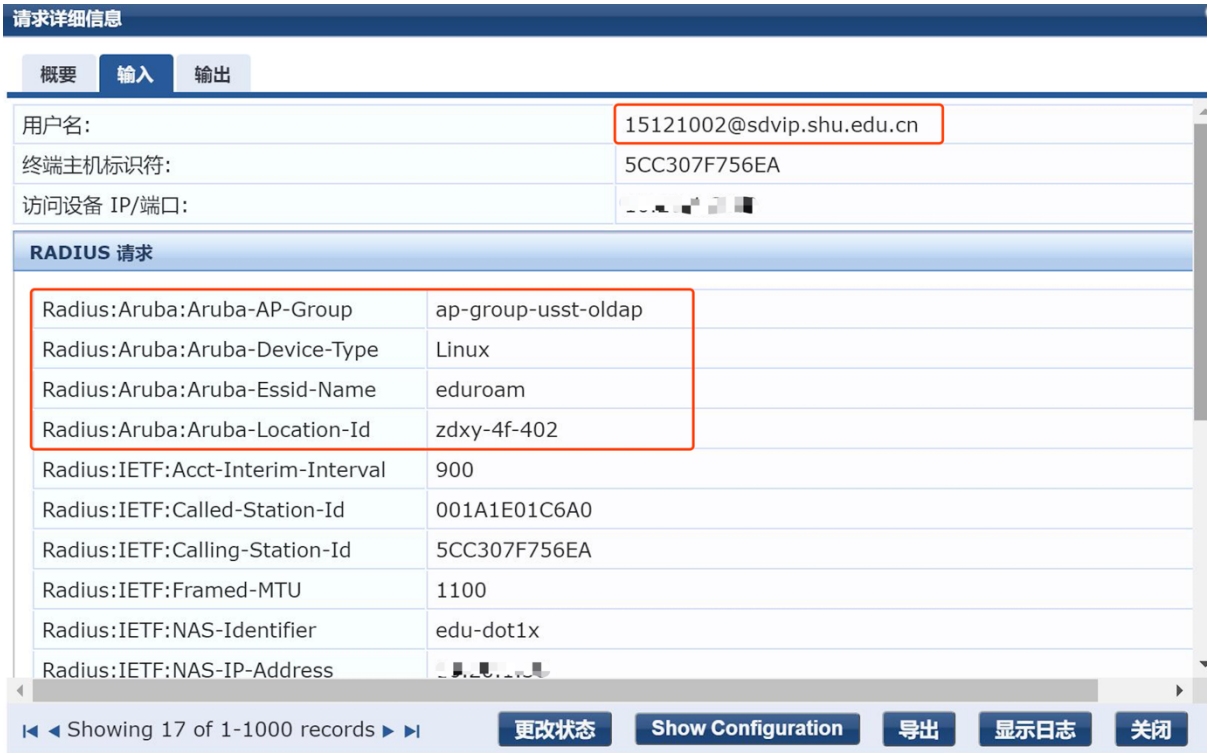


1.3.3 权限策略

- 同时在线设备小于 5 台的情况下，分配 eduroam 用户权限。

1.3.4 他校学生登录本校无线认证记录

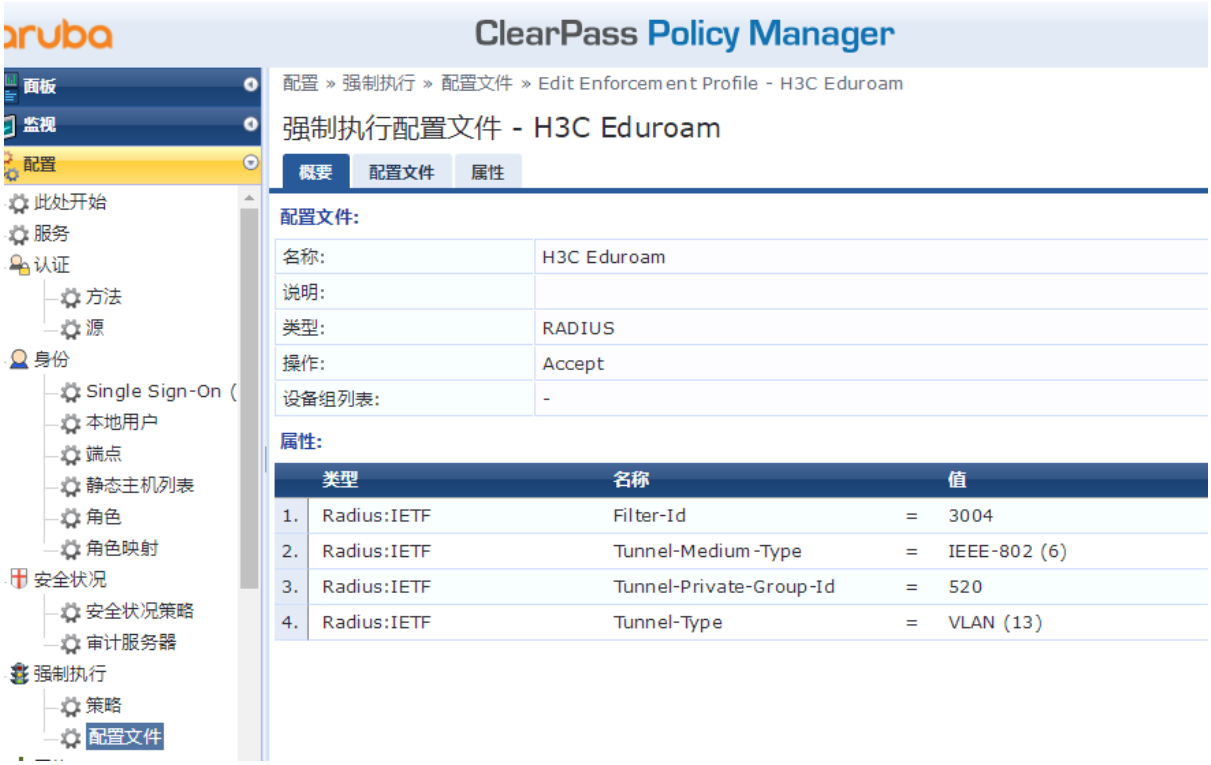
以下为上海大学学生登录我校无线的认证记录



2. 对接其他厂家的无线设备

2.1 对接其他厂商下发权限策略

ClearPass 除了对接 Aruba 无线控制器以外，还可以对接其他厂家的无线控制器，下面以 H3C 为例，H3C 区分权限的方式为基于 VLAN（相似的厂家还有思科，锐捷等）。认证入口和数据源都完全与前面所提到的完全一样，那就是说支持多种方式也不会让认证接口变得复杂。只需要在权限策略部分添加新的下发方式即可，如下：



2.2 自定义权限策略字典

ClearPass 还支持 Radius 权限策略字典的导入和定制化，在面对一些完全全新的厂家或独特的权限分配分类时，仅更新权限字典，并使用即可。如下：


滤器: 供应商名称
包含
Go
Clear Filter
供应商名称
供应商 ID
1. 3com
2. 3GPP
3. Acc
4. Acme
5. ADSL-Forum
6. Adva
7. Aerohive
8. Airespace
9. Alcatel
10. Alcatel-Luce
11. Alcatel-Luce
12. Alteon
13. Alvarion
14. APC
15. Aruba
RADIUS 属性
供应商名称:
Aerohive (26928)
属性名 ID 类型 入/出
1. AH-HM-Admin-Group-Id 1 Unsigned32 in out
Enable
导出
关闭