1 Table of Contents

Table of Contents

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
11 Nov 2019	0.1	Ariya Parsamanesh	Initial creation

2 Restricting Guest Captive Portal

Here in this short technote I'll show how to restrict the guest access from the corporate devices that are meant to connect to corporate dot1x wireless instead. This is a common requirement for organisation to restrict access for the corporate devices to connect to their guest WiFi network.

The main process in this solution is to add an attribute to the endpoint database in ClearPass for the corporate devices, when they connect to the dot1x wireless network for the first time. Then you can build an enforcement policy for guest service in ClearPass to block access for devices that have that endpoint database attribute.

2.1 Things you need

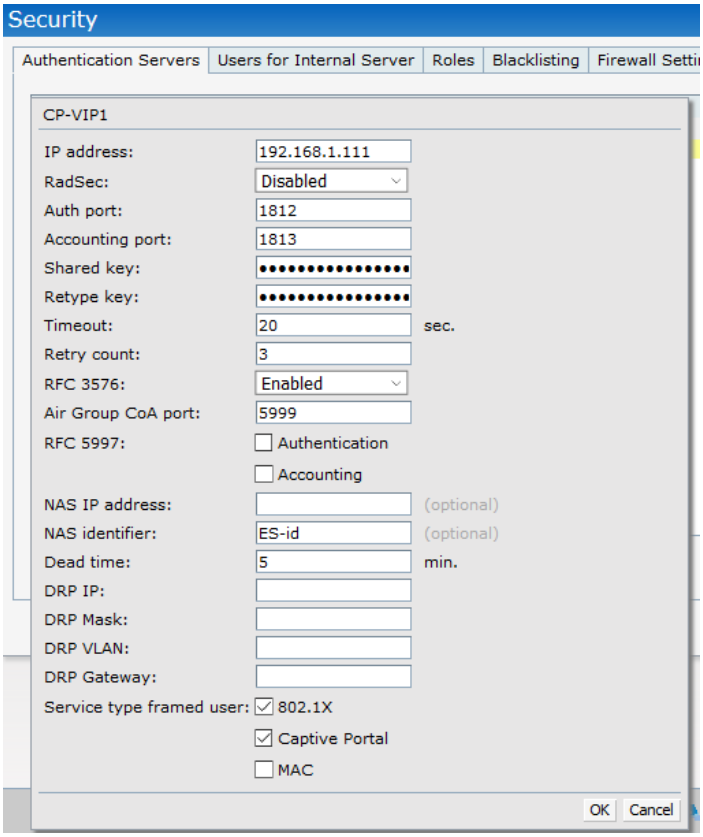
- Aruba Instant version 8.3. or later
- ClearPass 6.7 or later
- A Layer three switch

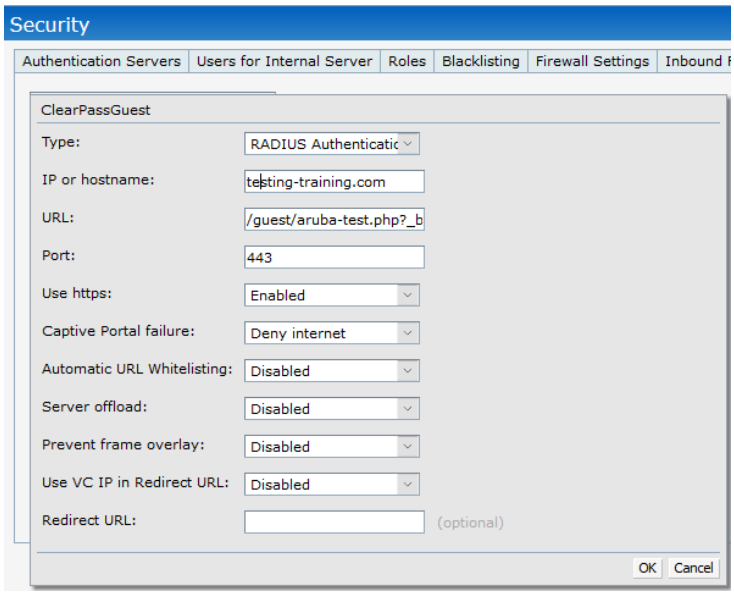
3 Instant AP Configuration

In this section we'll just create a dot1x and a guest service using ClearPass as the authentication server and external captive portal.

3.1 Authentication Server and Captive Portal Profile Configuration

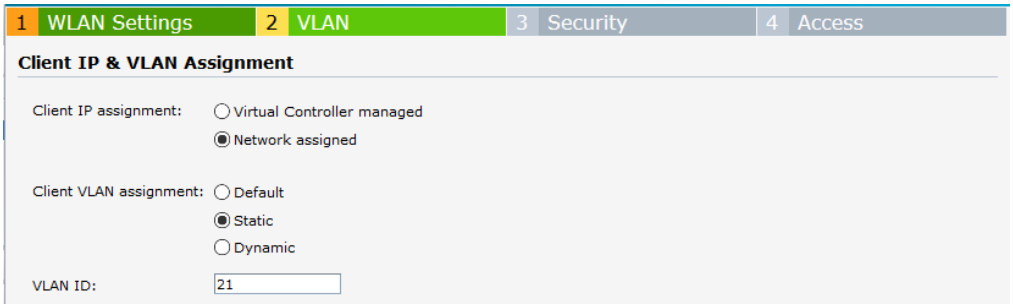
First we'll configure the RADIUS server.

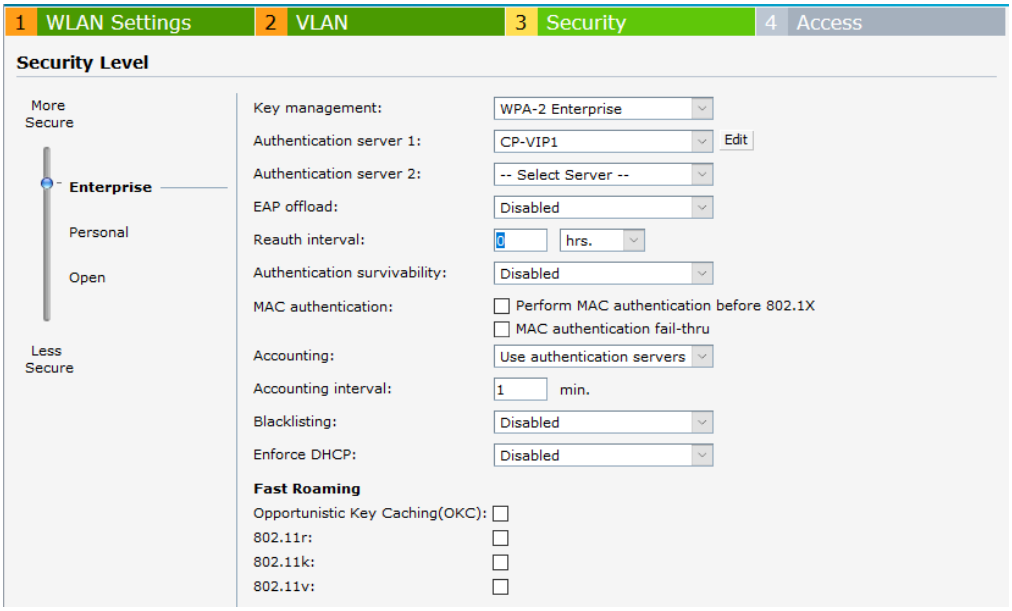


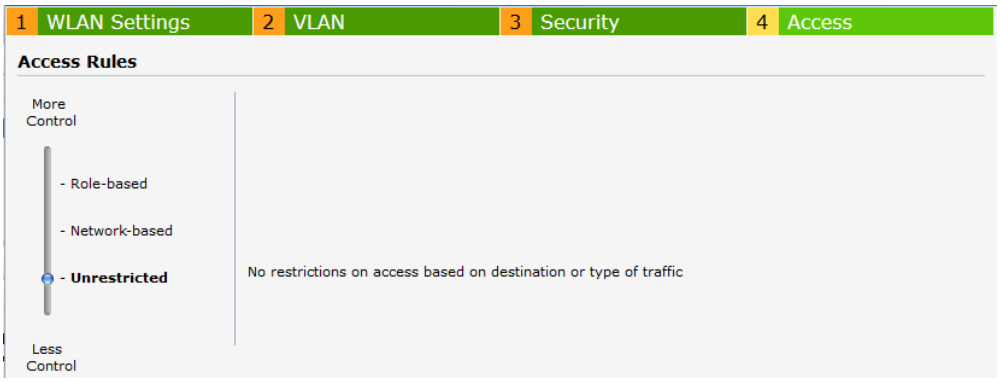


3.2 Dot1x WLAN Configuration

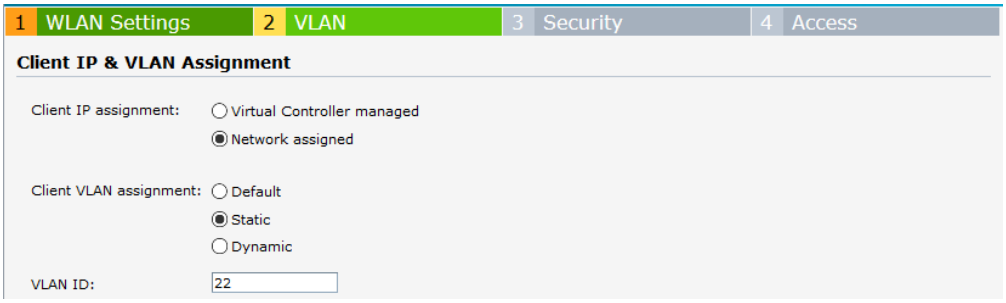
This is the classic dot1x wireless network configuration that I am showing here for completeness.

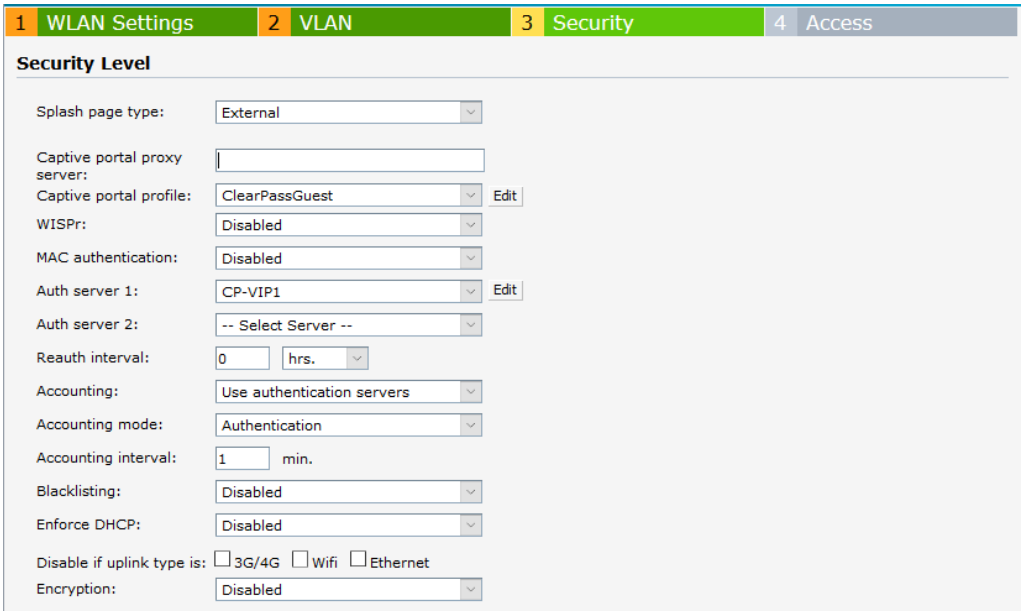


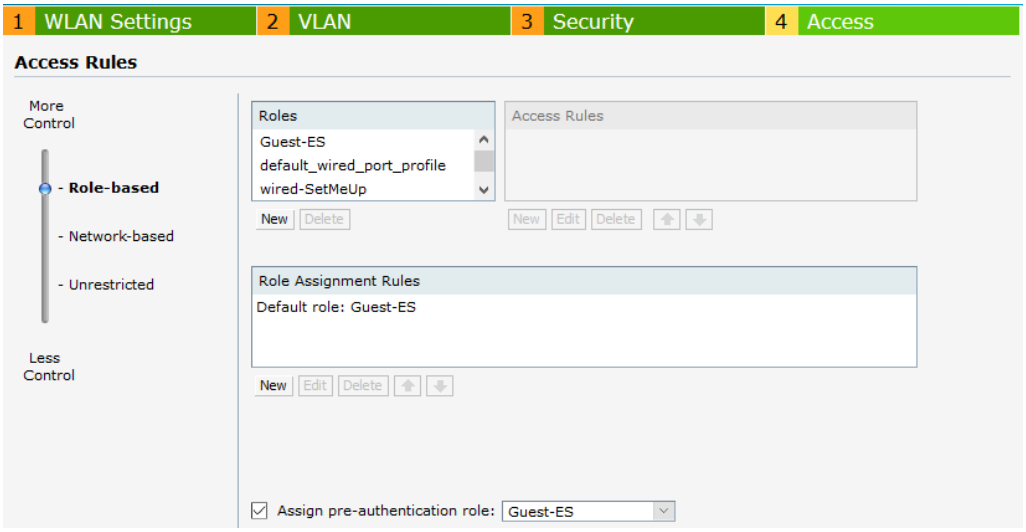




3.3 Guest WLAN Configuration




1 WLAN Settings
2 VLAN
3 Security
4 Access
Security Level
Splash page type: External
Captive portal proxy server:
Captive portal profile: ClearPassGuest Edit
WISPr: Disabled
MAC authentication: Disabled
Auth server 1: CP-VIP1 Edit
Auth server 2: -- Select Server --
Reauth interval: 0 hrs.
Accounting: Use authentication servers
Accounting mode: Authentication
Accounting interval: 1 min.
Blacklisting: Disabled
Enforce DHCP: Disabled
Disable if uplink type is: 3G/4G Wifi Ethernet
Encryption: Disabled


1 WLAN Settings
2 VLAN
3 Security
4 Access
Access Rules
More Control
- Role-based
- Network-based
- Unrestricted
Less Control
Roles
Guest-ES
default_wired_port_profile
wired-SetMeUp
New Delete
Access Rules
New Edit Delete
Role Assignment Rules
Default role: Guest-ES
New Edit Delete
Assign pre-authentication role: Guest-ES

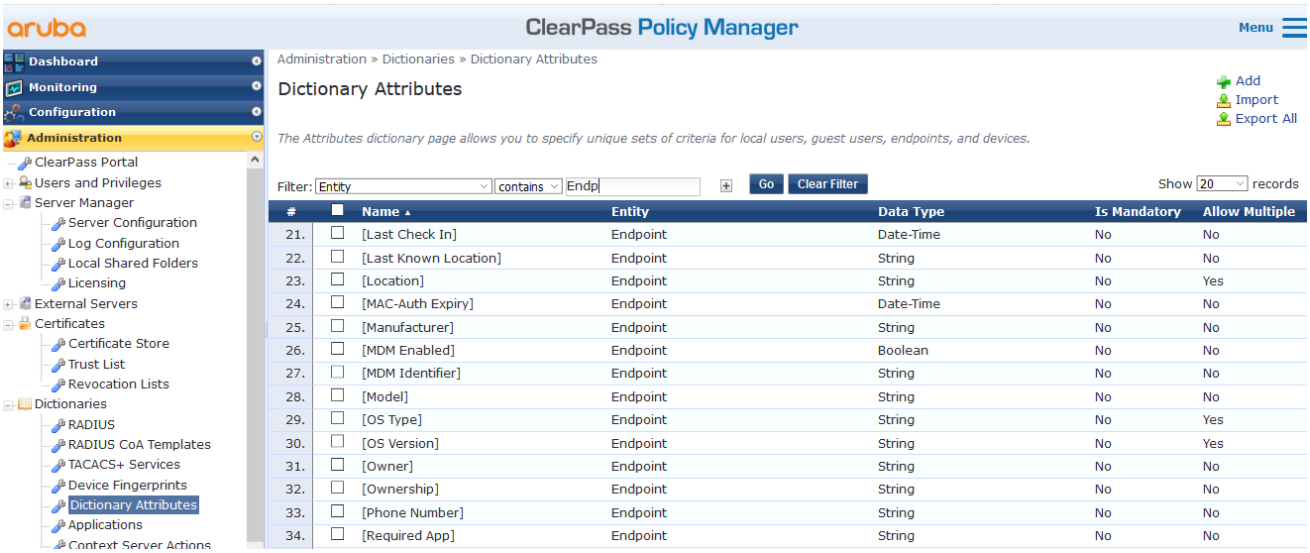
4 ClearPass dot1x Service Configuration

Here we'll cover the ClearPass Policy Manager configuration starting with the Enforcement Profiles. Also I am assuming ClearPass has joined the AD domain and an authentication source of type AD has been configured, so I am not showing those configurations.

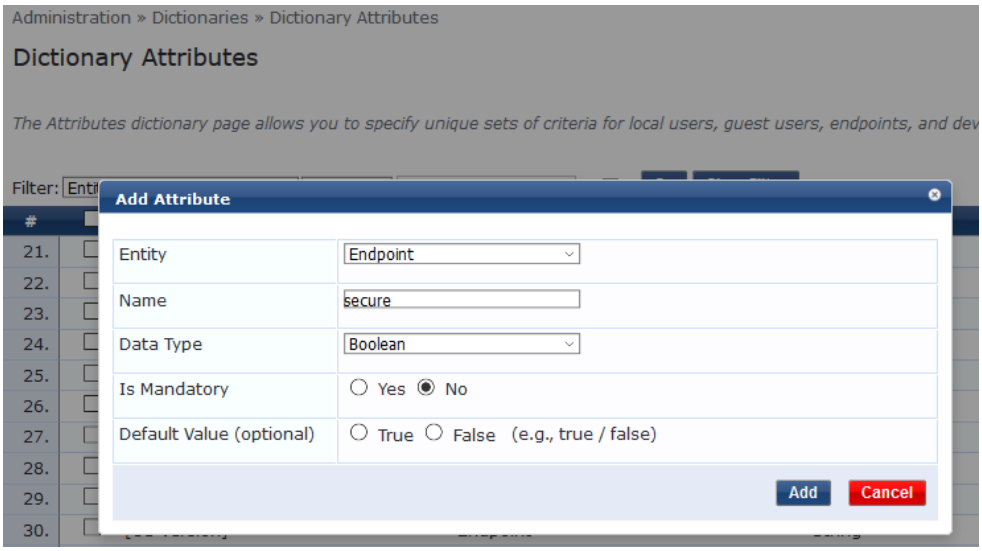
4.1 Endpoint Database Attribute

First we need to create a new attribute for the endpoint repository. Then we could reference this attribute in our enforcement profiles.

Go to Administration » Dictionaries » Dictionary Attributes and then filter on endpoint to see all the current attributes.



As you can see there are quite a few, about 53 attributes. We'll create an attribute called "secure".



This is the attribute that later on we'll use to check if the device was previously successfully connected to the dot1x network.

4.2 Enforcement Profiles

We are using 3x profiles,

1. aa Aruba 802.1X Wireless-Student
2. aa Aruba 802.1X Wireless-Staff
3. aa Aruba 802.1X Wireless Update Endpoint Secure

The first two enforcement profiles are of type RADIUS that sends back Aruba-user-role to the IAP. The last one is of type post-auth that updates an attribute in endpoint repository.

Summary | Profile | Attributes

Profile:

Name:	aa Aruba 802.1X Wireless-Student
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	student

Summary | Profile | Attributes

Profile:

Name:	aa Aruba 802.1X Wireless-Staff
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	staff

Summary | Profile | Attributes

Profile:

Name:	aa Aruba 802.1X Wireless Update Endpoint Secure
Description:	
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Endpoint	secure	=	true

4.3 Aruba 802.1X Wireless Service

Here is the dot1x service we are using.

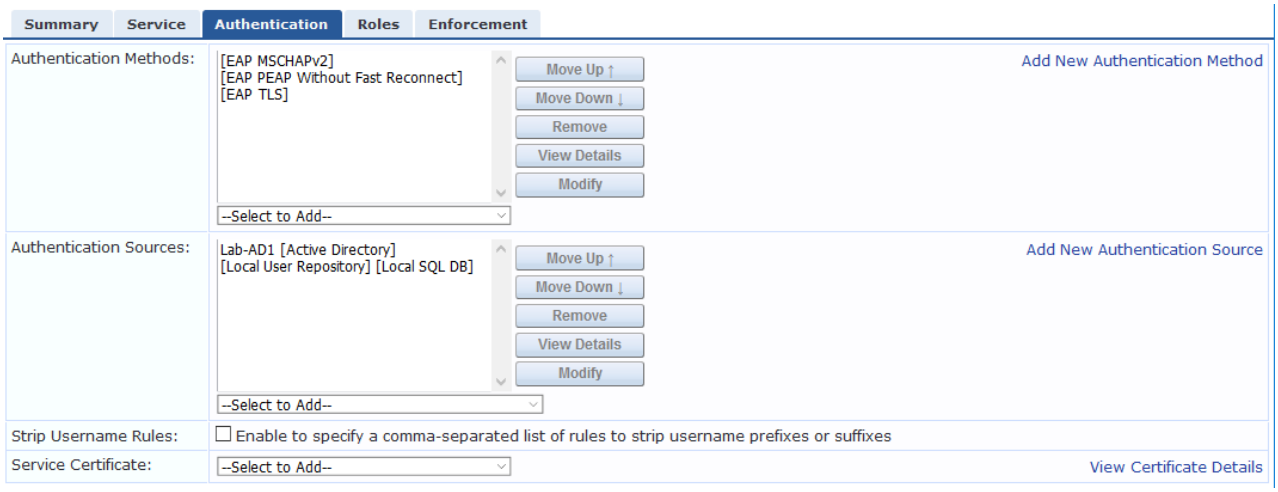
Summary | Service | Authentication | Roles | Enforcement

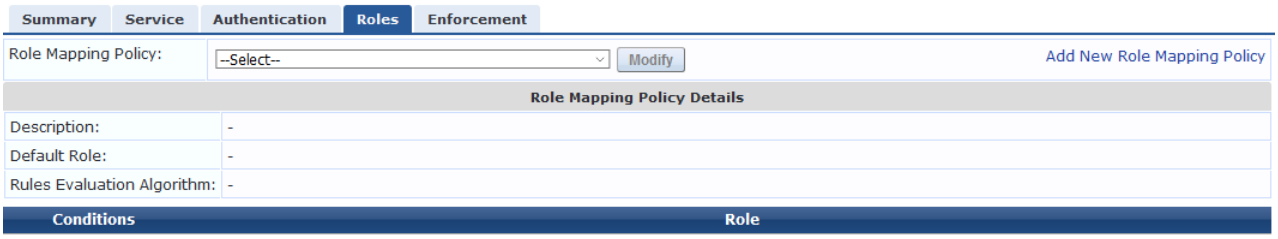
Name:	Aruba 802.1X Wireless
Description:	To authenticate users to an Aruba wireless network via 802.1X.
Type:	Aruba 802.1X Wireless
Status:	Enabled
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

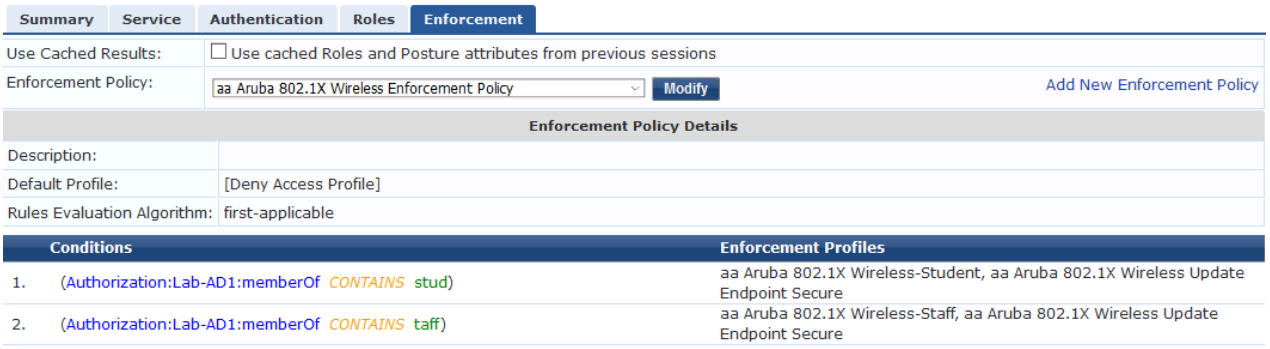
Service Rule

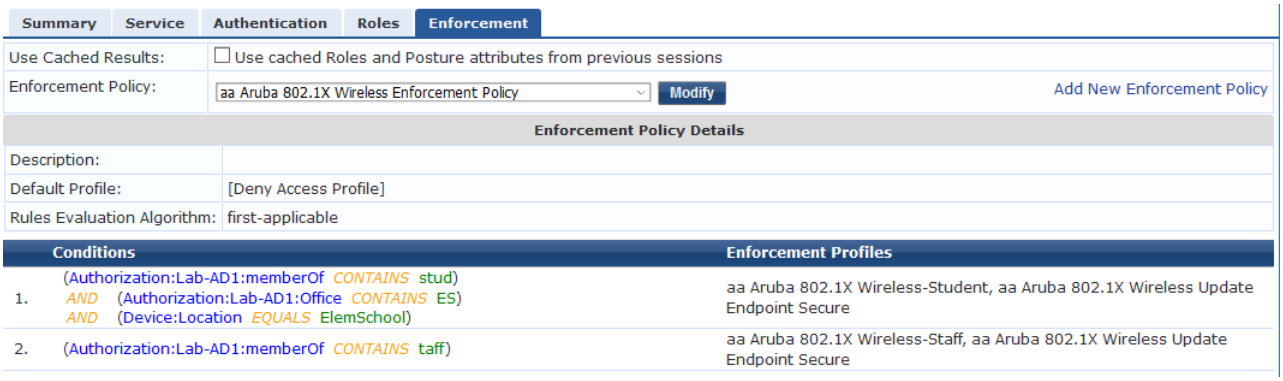
Matches ○ ANY or ◉ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Radius:Aruba	Aruba-Essid-Name	EXISTS	
4.	*Click to add...*			









Part of the enforcement policy we are updating the endpoint database by setting the “secure” attribute to true.

5 ClearPass Captive Portal Auth Service Configuration

Here we'll configure the captive portal authentication service that will be used for our guest users.

5.1 Enforcement Profiles

We are using 2x profiles, namely "aa Guest MAC_web" and "aa Guest MAC Caching".

Summary | Profile | Attributes

Profile:

Name:	aa Guest MAC_web
Description:	Role/VLAN enforcement for Guest
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	guest
2.	Radius:IETF	User-Name	=	%{Endpoint:Username}
3.	Radius:IETF	Session-Timeout	=	%{Authorization:[Guest User Repository]:RemainingExpiration}

aa Guest MAC Caching

Summary | Profile | Attributes

Profile:

Name:	aa Guest MAC Caching
Description:	Endpoint attribute updates for Guest
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Endpoint	Username	=	%{Authentication:Username}
2.	Endpoint	Guest Role ID	=	%{GuestUser:Role ID}
3.	Endpoint	MAC-Auth Expiry	=	%{Authorization:[Guest User Repository]:ExpireTime}

5.2 Captive Portal Authentication with MAC Caching Service

This is our MAC caching service.

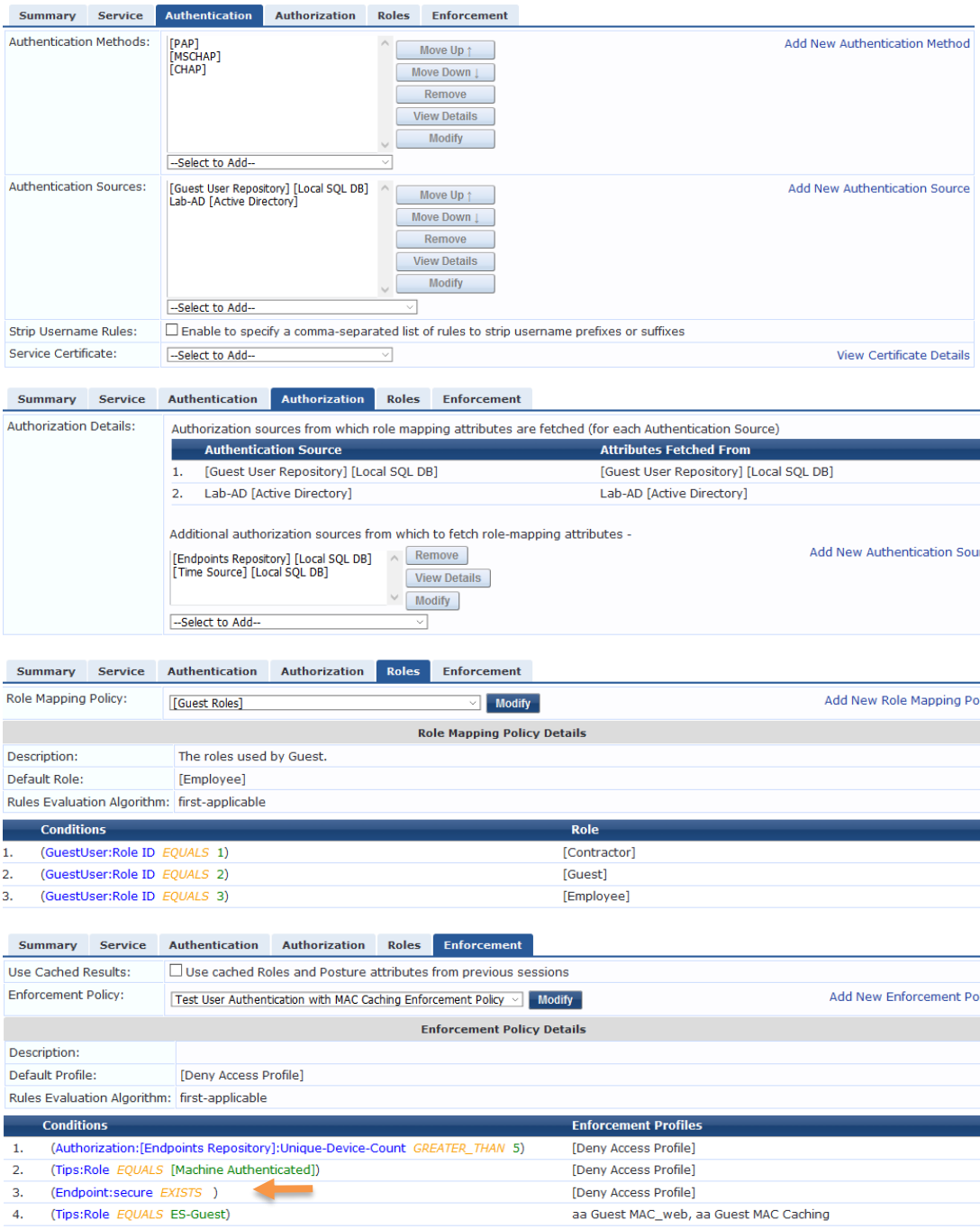
Summary | Service | Authentication | Authorization | Roles | Enforcement

Name:	Test CP Authentication with MAC Caching
Description:	Captive Portal authentication with MAC Caching
Type:	RADIUS Enforcement (Generic)
Status:	Enabled
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☑ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ○ ANY or ◉ ALL of the following conditions:

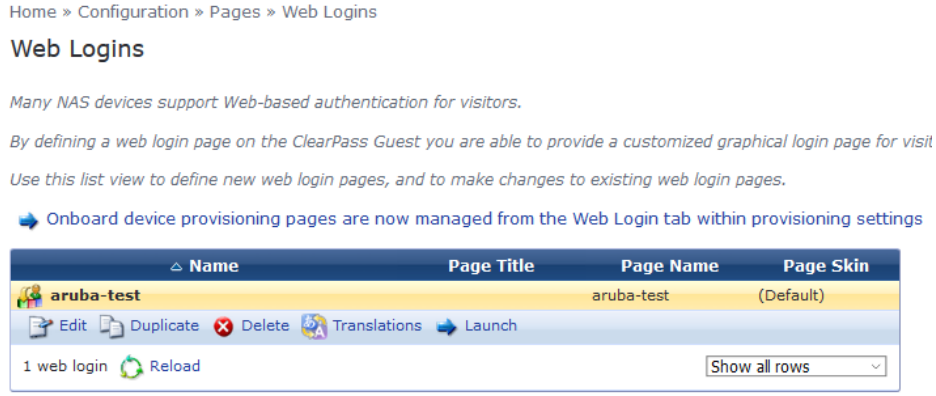
	Type	Name	Operator	Value
1.	Radius:IETF	Calling-Station-Id	EXISTS	
2.	Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}
3.	Radius:Aruba	Aruba-Essid-Name	CONTAINS	Guest
4.	*Click to add...*			



The important thing here is that we are checking for Endpoint attribute of “secure” and then based on that we are denying access.

5.3 ClearPass Guest Configuration

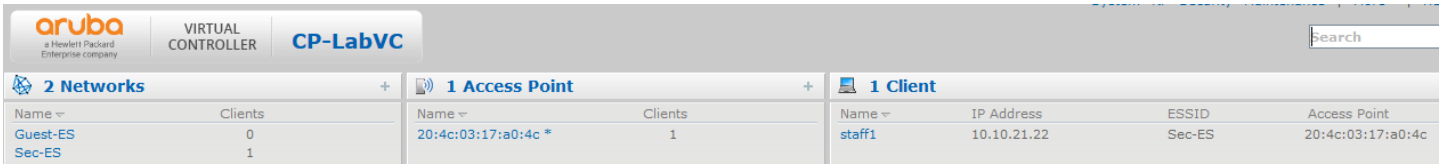
Here we have a very basic weblogin page for the guest redirection, hence I am not showing the detail of the page.



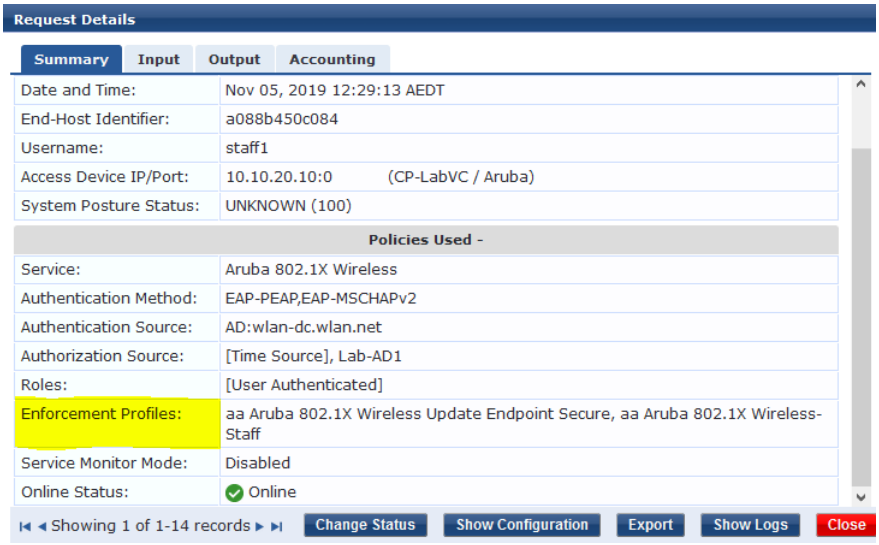
6 Demonstration -1

6.1 Dot1x Test for updating the Endpoint attribute

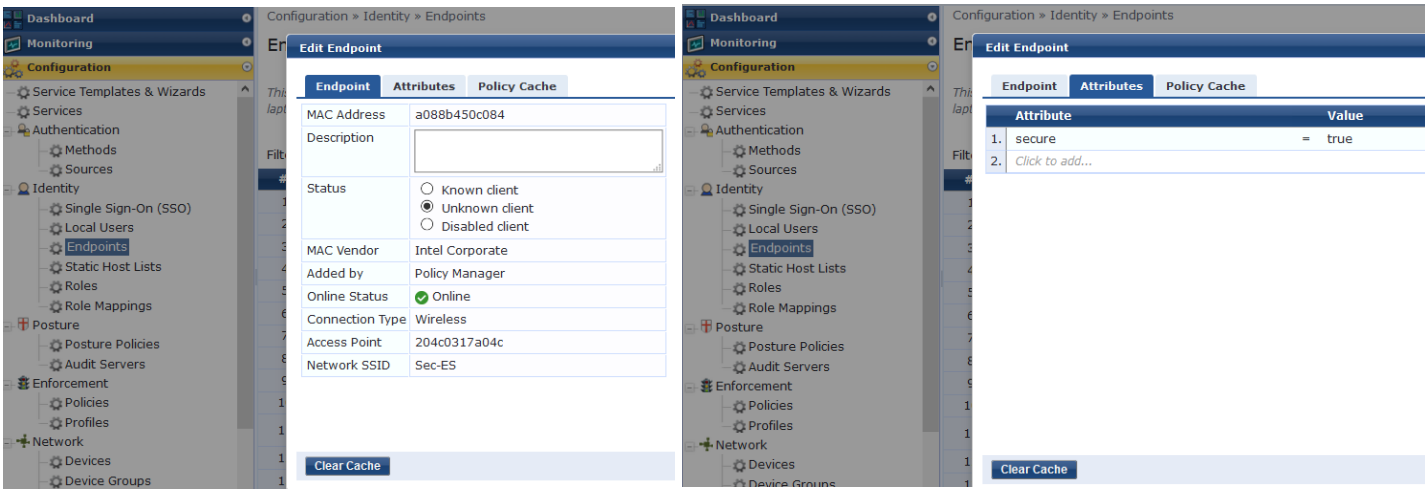
Now the client connects to the dot1x service with username staff1



Looking at the access tracker we see that it has matched the correct service and our enforcement profiles has been executed.



Next we go to endpoint database (Configuration » Identity » Endpoints) to see if the “secure” attribute has been updated.



As you can see above secure attribute is set to true.

6.2 Testing the Guest Service

At first we connect a valid guest user who had not successfully connected to the corporate/school dot1x wireless service. The user is first put into the pre-auth role.

aruba a Hewlett Packard Enterprise company | VIRTUAL CONTROLLER | CP-LabVC

2 Clients

Name	IP Address	MAC address	OS	ESSID	Access Point	Channel	Type	Role
--	10.10.22.20	a0:88:b4:50:c0:84	--	Guest-ES	20:4c:03:17:a0:4c	149+	AN	N/A
android-f3b06cc9a...	10.10.22.21	9c:02:98:8c:8a:47	Android	Guest-ES	20:4c:03:17:a0:4c	6	GN	Guest-ES

Then the client gets redirected to captive portal page and after using the valid guest credentials it can successfully login.

aruba ClearPass Guest

Please login to the network using your username and password.

Login

Username: cp@aa.com

Password: ••••••

Log In

Contact a staff member if you are experiencing difficulty logging in.

Here is the access tracker output for it.

Request Details

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R0000000d-01-5dc0d85b
Date and Time:	Nov 05, 2019 13:03:07 AEDT
End-Host Identifier:	9c02988c8a47 (SmartDevice / Android / Samsung Android)
Username:	cp@aa.com
Access Device IP/Port:	10.10.20.10:0 (CP-LabVC / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Test CP Authentication with MAC Caching
Authentication Method:	PAP
Authentication Source:	Local:localhost
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Guest], [User Authenticated]
Enforcement Profiles:	aa Guest MAC Caching, aa Guest MAC_web
Service Monitor Mode:	Disabled

Summary | Input | Output | Accounting

Enforcement Profiles:	aa Guest MAC Caching, aa Guest MAC_web
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Endpoint:Guest Role ID	2
Endpoint:MAC-Auth Expiry	2019-11-05 16:44:22
Endpoint:Username	cp@aa.com
Radius:Aruba:Aruba-User-Role	guest
Radius:IETF:Session-Timeout	13274
Radius:IETF:User-Name	cp@aa.com

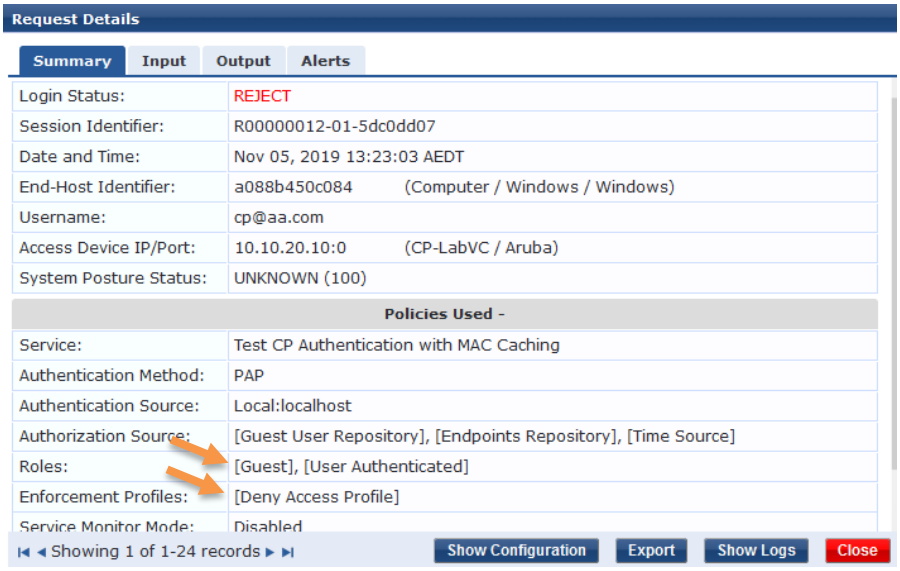
Note here the user role has changed to “guest”

aruba a Hewlett Packard Enterprise company | VIRTUAL CONTROLLER | CP-LabVC

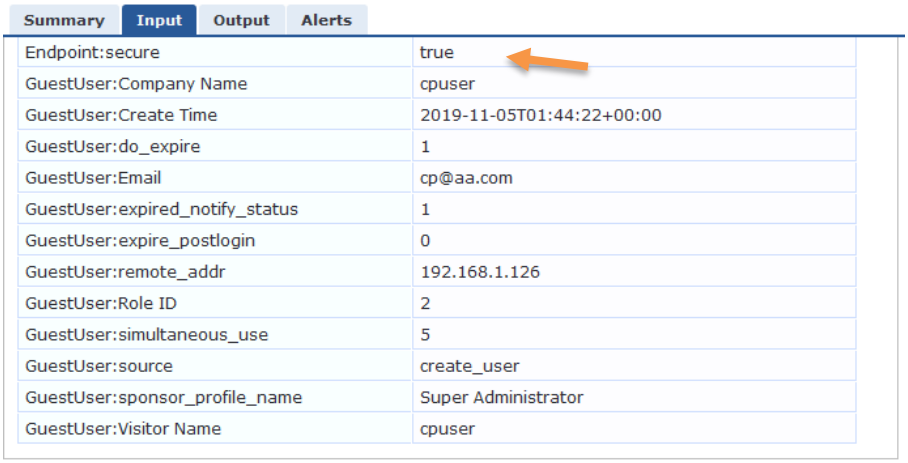
2 Clients

Name	IP Address	MAC address	OS	ESSID	Access Point	Channel	Type	Role
--	10.10.22.20	a0:88:b4:50:c0:84	--	Guest-ES	20:4c:03:17:a0:4c	149+	AN	N/A
cp@aa.com	10.10.22.21	9c:02:98:8c:8a:47	Android	Guest-ES	20:4c:03:17:a0:4c	6	GN	guest

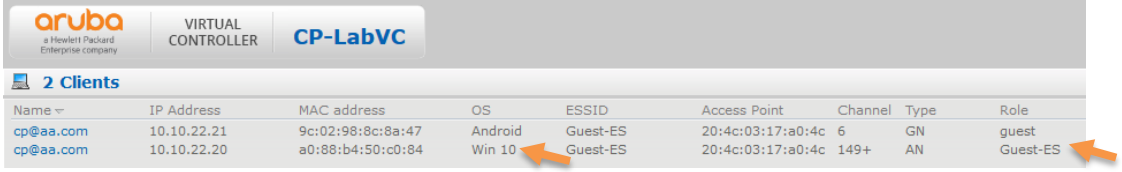
Now we'll login with a corporate owned device to the guest network. And use a valid guest credential to login (cp@aa.com)



Note here that the user has successfully authenticated but the authorisation will deny access for this client. Checking the computed attributes shows the guest account details that was used.



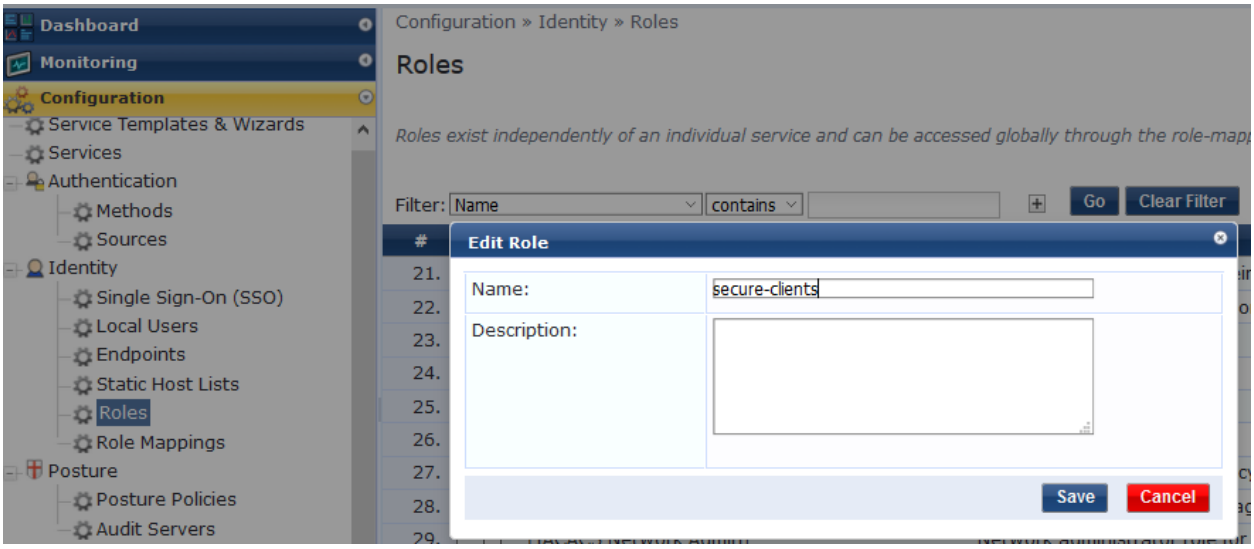
And looking at the Instant AP, we see that the second cp@aa.com "guest" user is stuck in pre-auth user role.



7 Demonstration -2

Here we'll change the logic in the "Test CP Authentication with MAC Caching" service to use the use role mapping instead.

First we need to create a user role called "secure-clients"



Then we'll create a new role mapping policy.

Summary | Policy | Mapping Rules

Policy:

Policy Name:	Guest-roles
Description:	The roles used by Guest.
Default Role:	[Other]

Mapping Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Role Name
1.	(Endpoint:secure *EQUALS* true)	secure-clients

Next we'll use this role mapping policy in our "Test CP Authentication with MAC Caching" service

Summary | Service | Authentication | Authorization | Roles | Enforcement

Role Mapping Policy: Guest-roles Modify Add New Role Mapping Policy

Role Mapping Policy Details

Description:	The roles used by Guest.
Default Role:	[Other]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Role
1.	(Endpoint:secure *EQUALS* true)	secure-clients

Finally modifying our enforcement policy to use Tips:role .

Summary | Service | Authentication | Authorization | Roles | Enforcement

Use Cached Results: Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Test User Authentication with MAC Caching Enforcement Policy Modify Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	aa Aruba 802.1X Wireless-Employee
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* secure-clients)	[Deny Access Profile]
2.	(Authorization:[Endpoints Repository]:Unique-Device-Count *GREATER_THAN* 5)	[Deny Access Profile]
3.	(Tips:Role *EQUALS* [Machine Authenticated])	[Deny Access Profile]
4.	(Tips:Role *EQUALS* [Guest])	aa Guest MAC_web, aa Guest MAC Caching

Make sure you save the changed and now we are ready to test it again.

7.1 Testing with Role-Mapping Approach

We have reconnected the win10 laptop to the guest SSID and the client gets redirected to the login page, where we'll use the same credentials as a valid guest to login.

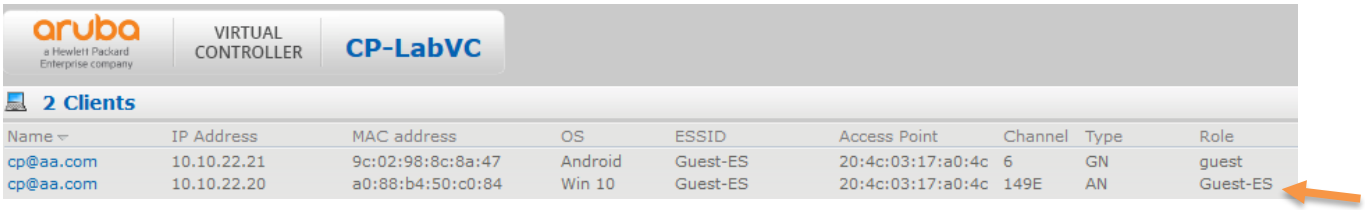
Here is the access tracker output.

Summary | Input | Output | Alerts

Login Status:	REJECT
Session Identifier:	R00000017-01-5dc0e814
Date and Time:	Nov 05, 2019 14:10:12 AEDT
End-Host Identifier:	a088b450c084 (Computer / Windows / Windows)
Username:	cp@aa.com
Access Device IP/Port:	10.10.20.10:0 (CP-LabVC / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Test CP Authentication with MAC Caching
Authentication Method:	PAP
Authentication Source:	Local:localhost
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Guest], [User Authenticated], secure-clients
Enforcement Profiles:	[Deny Access Profile]
Service Monitor Mode:	Disabled

You can see the user has matched three roles, [Guest], [User Authenticated] and secure-clients.

And since we are matching on "secure-clients" and denying access the login status is rejected and when you look at the Instant AP, the win10 client is stuck in "Guest-ES" role.



Name	IP Address	MAC address	OS	ESSID	Access Point	Channel	Type	Role
cp@aa.com	10.10.22.21	9c:02:98:8c:8a:47	Android	Guest-ES	20:4c:03:17:a0:4c	6	GN	guest
cp@aa.com	10.10.22.20	a0:88:b4:50:c0:84	Win 10	Guest-ES	20:4c:03:17:a0:4c	149E	AN	Guest-ES