

# 1 Table of Contents

---

## Table of Contents

1	Table of Contents .....	1
1.1	Revision History .....	1
2	Restricting Guest Captive Portal.....	2
2.1	Things you need .....	2
3	Instant AP Configuration.....	3
3.1	Authentication Server and Captive Portal Profile Configuration .....	3
3.2	Dot1x WLAN Configuration .....	3
3.3	Guest WLAN Configuration .....	4
4	ClearPass dot1x Service Configuration.....	6
4.1	Endpoint Database Attribute .....	6
4.2	Enforcement Profiles.....	6
4.3	Aruba 802.1X Wireless Service .....	7
5	ClearPass Captive Portal Auth Service Configuration.....	9
5.1	Enforcement Profiles.....	9
5.2	Captive Portal Authentication with MAC Caching Service .....	9
5.3	ClearPass Guest Configuration .....	10
6	Demonstration -1 .....	11
6.1	Dot1x Test for updating the Endpoint attribute .....	11
6.2	Testing the Guest Service .....	11
7	Demonstration -2 .....	14
7.1	Testing with Role-Mapping Approach .....	15

## 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.

The left screenshot shows the 'Security' configuration window with the 'Authentication Servers' sub-tab selected. It displays the configuration for 'CP-VIP1'. The configuration includes fields for IP address (192.168.1.111), RadSec (Disabled), Auth port (1812), Accounting port (1813), Shared key, Retype key, Timeout (20 sec), Retry count (3), RFC 3576 (Enabled), Air Group CoA port (5999), RFC 5997 (Authentication and Accounting), NAS IP address, NAS identifier (ES-id), Dead time (5 min), and various DHCP options (DRP IP, Mask, VLAN, Gateway). Service type framed user options include 802.1X, Captive Portal, and MAC.

The right screenshot shows the 'Security' configuration window with the 'Users for Internal Server' sub-tab selected. It displays the configuration for 'ClearPassGuest'. The configuration includes fields for Type (RADIUS Authentication), IP or hostname (testing-training.com), URL (/guest/aruba-test.php?\_b), Port (443), Use https (Enabled), Captive Portal failure (Deny internet), Automatic URL Whitelisting (Disabled), Server offload (Disabled), Prevent frame overlay (Disabled), Use VC IP in Redirect URL (Disabled), and Redirect URL (optional).

### 3.2 Dot1x WLAN Configuration

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

The left screenshot shows the 'Edit Sec-ES' configuration window with the 'WLAN Settings' tab selected. It displays the configuration for 'Sec-ES'. The configuration includes fields for Name & Usage, Name (Sec-ES), Primary usage (Employee, Voice, Guest), and Client IP assignment (Virtual Controller managed, Network assigned). Client VLAN assignment options include Default, Static, and Dynamic. The VLAN ID is set to 21.

The right screenshot shows the 'Edit Sec-ES' configuration window with the 'VLAN' tab selected. It displays the configuration for 'Client IP & VLAN Assignment'. The configuration includes fields for Client IP assignment (Virtual Controller managed, Network assigned), Client VLAN assignment (Default, Static, Dynamic), and VLAN ID (21).

1 WLAN Settings
2 VLAN
3 Security
4 Access

### Security Level

More Secure  
Less Secure

Enterprise  
Personal  
Open

Key management: WPA-2 Enterprise  
Authentication server 1: CP-VIP1 [Edit](#)  
Authentication server 2: -- Select Server --  
EAP offload: Disabled  
Reauth interval: 0 hrs.  
Authentication survivability: Disabled  
MAC authentication:  
☐ Perform MAC authentication before 802.1X  
☐ MAC authentication fail-thru  
Accounting: Use authentication servers  
Accounting interval: 1 min.  
Blacklisting: Disabled  
Enforce DHCP: Disabled  
**Fast Roaming**  
Opportunistic Key Caching(OKC): ☐  
802.11r: ☐  
802.11k: ☐  
802.11v: ☐

1 WLAN Settings
2 VLAN
3 Security
4 Access

### Access Rules

More Control  
Less Control

- Role-based  
- Network-based  
- **Unrestricted**

No restrictions on access based on destination or type of traffic

## 3.3 Guest WLAN Configuration

Edit Guest-ES [Help](#)

1 WLAN Settings
2 VLAN
3 Security
4 Access

### WLAN Settings

Name & Usage

Name: Guest-ES  
Primary usage: ☐ Employee  
☐ Voice  
☒ Guest

1 WLAN Settings
2 VLAN
3 Security
4 Access

### Client IP & VLAN Assignment

Client IP assignment: ☐ Virtual Controller managed  
☒ Network assigned  
Client VLAN assignment: ☐ Default  
☒ Static  
☐ Dynamic  
VLAN ID: 22

## 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

## 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

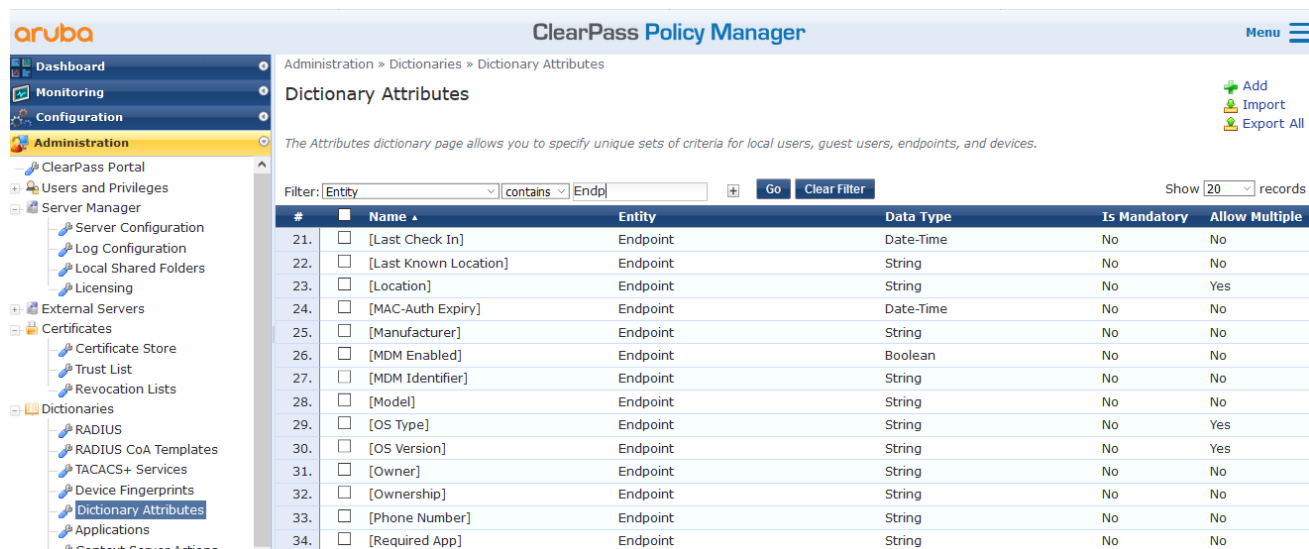
## 4 ClearPass dot1x Service Configuration

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.



#	Name	Entity	Data Type	Is Mandatory	Allow Multiple
21.	[Last Check In]	Endpoint	Date-Time	No	No
22.	[Last Known Location]	Endpoint	String	No	No
23.	[Location]	Endpoint	String	No	Yes
24.	[MAC-Auth Expiry]	Endpoint	Date-Time	No	No
25.	[Manufacturer]	Endpoint	String	No	No
26.	[MDM Enabled]	Endpoint	Boolean	No	No
27.	[MDM Identifier]	Endpoint	String	No	No
28.	[Model]	Endpoint	String	No	No
29.	[OS Type]	Endpoint	String	No	Yes
30.	[OS Version]	Endpoint	String	No	Yes
31.	[Owner]	Endpoint	String	No	No
32.	[Ownership]	Endpoint	String	No	No
33.	[Phone Number]	Endpoint	String	No	No
34.	[Required App]	Endpoint	String	No	No

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



Administration » Dictionaries » Dictionary Attributes

Dictionary Attributes

The Attributes dictionary page allows you to specify unique sets of criteria for local users, guest users, endpoints, and devices.

Filter: Entity contains Endp Go Clear Filter Show 20 records

**Add Attribute**

Entity: Endpoint

Name: secure

Data Type: Boolean

Is Mandatory: ☐ Yes ☒ No

Default Value (optional): ☐ True ☒ False (e.g., true / false)

Add Cancel

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
<b>Profile:</b>		
Name:	aa Aruba 802.1X Wireless-Student	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
<b>Attributes:</b>		
Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= student

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	aa Aruba 802.1X Wireless-Staff	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
<b>Attributes:</b>		
Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= staff

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	aa Aruba 802.1X Wireless Update Endpoint Secure	
Description:		
Type:	Post_Authentication	
Action:		
Device Group List:	-	
<b>Attributes:</b>		
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:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy			
<b>Service Rule</b>				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> 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. <a href="#">Click to add...</a>				

Summary	Service	Authentication	Roles	Enforcement
Authentication Methods: [EAP MSCHAPv2] [EAP PEAP Without Fast Reconnect] [EAP TLS] <div>             Move Up ↑              Move Down ↓              Remove              View Details              Modify           </div> --Select to Add-- <a href="#">Add New Authentication Method</a>				
Authentication Sources: Lab-AD1 [Active Directory] [Local User Repository] [Local SQL DB] <div>             Move Up ↑              Move Down ↓              Remove              View Details              Modify           </div> --Select to Add-- <a href="#">Add New Authentication Source</a>				
Strip Username Rules: <input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes				
Service Certificate: --Select to Add-- <a href="#">View Certificate Details</a>				

Summary	Service	Authentication	Roles	Enforcement				
Role Mapping Policy: --Select-- <a href="#">Modify</a> <a href="#">Add New Role Mapping Policy</a>								
Role Mapping Policy Details								
Description: -								
Default Role: -								
Rules Evaluation Algorithm: -								
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td colspan="2"> </td> </tr> </tbody> </table>					Conditions	Role		
Conditions	Role							

Summary	Service	Authentication	Roles	Enforcement						
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions										
Enforcement Policy: aa Aruba 802.1X Wireless Enforcement Policy <a href="#">Modify</a> <a href="#">Add New Enforcement Policy</a>										
Enforcement Policy Details										
Description:										
Default Profile: [Deny Access Profile]										
Rules Evaluation Algorithm: first-applicable										
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Enforcement Profiles</th> </tr> </thead> <tbody> <tr> <td>1. (Authorization:Lab-AD1:memberOf CONTAINS stud)</td> <td>aa Aruba 802.1X Wireless-Student, aa Aruba 802.1X Wireless Update Endpoint Secure</td> </tr> <tr> <td>2. (Authorization:Lab-AD1:memberOf CONTAINS taff)</td> <td>aa Aruba 802.1X Wireless-Staff, aa Aruba 802.1X Wireless Update Endpoint Secure</td> </tr> </tbody> </table>					Conditions	Enforcement Profiles	1. (Authorization:Lab-AD1:memberOf CONTAINS stud)	aa Aruba 802.1X Wireless-Student, aa Aruba 802.1X Wireless Update Endpoint Secure	2. (Authorization:Lab-AD1:memberOf CONTAINS taff)	aa Aruba 802.1X Wireless-Staff, aa Aruba 802.1X Wireless Update Endpoint Secure
Conditions	Enforcement Profiles									
1. (Authorization:Lab-AD1:memberOf CONTAINS stud)	aa Aruba 802.1X Wireless-Student, aa Aruba 802.1X Wireless Update Endpoint Secure									
2. (Authorization:Lab-AD1:memberOf CONTAINS taff)	aa Aruba 802.1X Wireless-Staff, aa Aruba 802.1X Wireless Update Endpoint Secure									

Summary	Service	Authentication	Roles	Enforcement						
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions										
Enforcement Policy: aa Aruba 802.1X Wireless Enforcement Policy <a href="#">Modify</a> <a href="#">Add New Enforcement Policy</a>										
Enforcement Policy Details										
Description:										
Default Profile: [Deny Access Profile]										
Rules Evaluation Algorithm: first-applicable										
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Enforcement Profiles</th> </tr> </thead> <tbody> <tr> <td>1. (Authorization:Lab-AD1:memberOf CONTAINS stud) AND (Authorization:Lab-AD1:Office CONTAINS ES) AND (Device:Location EQUALS ElemSchool)</td> <td>aa Aruba 802.1X Wireless-Student, aa Aruba 802.1X Wireless Update Endpoint Secure</td> </tr> <tr> <td>2. (Authorization:Lab-AD1:memberOf CONTAINS taff)</td> <td>aa Aruba 802.1X Wireless-Staff, aa Aruba 802.1X Wireless Update Endpoint Secure</td> </tr> </tbody> </table>					Conditions	Enforcement Profiles	1. (Authorization:Lab-AD1:memberOf CONTAINS stud) AND (Authorization:Lab-AD1:Office CONTAINS ES) AND (Device:Location EQUALS ElemSchool)	aa Aruba 802.1X Wireless-Student, aa Aruba 802.1X Wireless Update Endpoint Secure	2. (Authorization:Lab-AD1:memberOf CONTAINS taff)	aa Aruba 802.1X Wireless-Staff, aa Aruba 802.1X Wireless Update Endpoint Secure
Conditions	Enforcement Profiles									
1. (Authorization:Lab-AD1:memberOf CONTAINS stud) AND (Authorization:Lab-AD1:Office CONTAINS ES) AND (Device:Location EQUALS ElemSchool)	aa Aruba 802.1X Wireless-Student, aa Aruba 802.1X Wireless Update Endpoint Secure									
2. (Authorization:Lab-AD1:memberOf CONTAINS taff)	aa Aruba 802.1X Wireless-Staff, aa Aruba 802.1X Wireless Update Endpoint Secure									

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		
<b>Profile:</b>				
Name:	aa Guest MAC_web			
Description:	Role/VLAN enforcement for Guest			
Type:	RADIUS			
Action:	Accept			
Device Group List:	-			
<b>Attributes:</b>				
	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:	<div>Test CP Authentication with MAC Caching</div>				
Description:	<div>Captive Portal authentication with MAC Caching</div>				
Type:	RADIUS Enforcement ( Generic )				
Status:	Enabled				
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement				
More Options:	<input checked="" type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy				
Service Rule					
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> 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. <a href="#">Click to add...</a>					

Summary	Service	Authentication	Authorization	Roles	Enforcement
Authentication Methods: [PAP] [MSCHAP] [CHAP] <span style="float: right;">Add New Authentication Method</span> <div style="float: right; text-align: right;">             Move Up ↑              Move Down ↓              Remove              View Details              Modify           </div>					
Authentication Sources: [Guest User Repository] [Local SQL DB] [Lab-AD] [Active Directory] <span style="float: right;">Add New Authentication Source</span> <div style="float: right; text-align: right;">             Move Up ↑              Move Down ↓              Remove              View Details              Modify           </div>					
Strip Username Rules: <input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes					
Service Certificate: --Select to Add-- <span style="float: right;">View Certificate Details</span>					

Summary	Service	Authentication	Authorization	Roles	Enforcement						
Authorization Details: Authorization sources from which role mapping attributes are fetched (for each Authentication Source)											
<table border="1"> <thead> <tr> <th>Authentication Source</th> <th>Attributes Fetched From</th> </tr> </thead> <tbody> <tr> <td>1. [Guest User Repository] [Local SQL DB]</td> <td>[Guest User Repository] [Local SQL DB]</td> </tr> <tr> <td>2. Lab-AD [Active Directory]</td> <td>Lab-AD [Active Directory]</td> </tr> </tbody> </table>						Authentication Source	Attributes Fetched From	1. [Guest User Repository] [Local SQL DB]	[Guest User Repository] [Local SQL DB]	2. Lab-AD [Active Directory]	Lab-AD [Active Directory]
Authentication Source	Attributes Fetched From										
1. [Guest User Repository] [Local SQL DB]	[Guest User Repository] [Local SQL DB]										
2. Lab-AD [Active Directory]	Lab-AD [Active Directory]										
Additional authorization sources from which to fetch role-mapping attributes - <span style="float: right;">Add New Authentication Source</span> <div style="float: right; text-align: right;">             Remove              View Details              Modify           </div>											
[Endpoints Repository] [Local SQL DB] [Time Source] [Local SQL DB]											
--Select to Add--											

Summary	Service	Authentication	Authorization	Roles	Enforcement								
Role Mapping Policy: [Guest Roles] <span style="float: right;">Add New Role Mapping Policy</span>													
<div style="text-align: center;">Role Mapping Policy Details</div>													
Description: The roles used by Guest.													
Default Role: [Employee]													
Rules Evaluation Algorithm: first-applicable													
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td>1. (GuestUser:Role ID EQUALS 1)</td> <td>[Contractor]</td> </tr> <tr> <td>2. (GuestUser:Role ID EQUALS 2)</td> <td>[Guest]</td> </tr> <tr> <td>3. (GuestUser:Role ID EQUALS 3)</td> <td>[Employee]</td> </tr> </tbody> </table>						Conditions	Role	1. (GuestUser:Role ID EQUALS 1)	[Contractor]	2. (GuestUser:Role ID EQUALS 2)	[Guest]	3. (GuestUser:Role ID EQUALS 3)	[Employee]
Conditions	Role												
1. (GuestUser:Role ID EQUALS 1)	[Contractor]												
2. (GuestUser:Role ID EQUALS 2)	[Guest]												
3. (GuestUser:Role ID EQUALS 3)	[Employee]												

Summary	Service	Authentication	Authorization	Roles	Enforcement										
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions															
Enforcement Policy: [Test User Authentication with MAC Caching Enforcement Policy] <span style="float: right;">Add New Enforcement Policy</span>															
<div style="text-align: center;">Enforcement Policy Details</div>															
Description:															
Default Profile: [Deny Access Profile]															
Rules Evaluation Algorithm: first-applicable															
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Enforcement Profiles</th> </tr> </thead> <tbody> <tr> <td>1. (Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 5)</td> <td>[Deny Access Profile]</td> </tr> <tr> <td>2. (Tips:Role EQUALS [Machine Authenticated])</td> <td>[Deny Access Profile]</td> </tr> <tr> <td>3. (Endpoint:secure EXISTS )</td> <td>[Deny Access Profile]</td> </tr> <tr> <td>4. (Tips:Role EQUALS ES-Guest)</td> <td>aa Guest MAC_web, aa Guest MAC Caching</td> </tr> </tbody> </table>						Conditions	Enforcement Profiles	1. (Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 5)	[Deny Access Profile]	2. (Tips:Role EQUALS [Machine Authenticated])	[Deny Access Profile]	3. (Endpoint:secure EXISTS )	[Deny Access Profile]	4. (Tips:Role EQUALS ES-Guest)	aa Guest MAC_web, aa Guest MAC Caching
Conditions	Enforcement Profiles														
1. (Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 5)	[Deny Access Profile]														
2. (Tips:Role EQUALS [Machine Authenticated])	[Deny Access Profile]														
3. (Endpoint:secure EXISTS )	[Deny Access Profile]														
4. (Tips:Role EQUALS ES-Guest)	aa Guest MAC_web, aa Guest MAC Caching														

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.

Home » Configuration » Pages » Web Logins

### Web Logins

Many NAS devices support Web-based authentication for visitors.

By defining a web login page on the ClearPass Guest you are able to provide a customized graphical login page for visit

Use this list view to define new web login pages, and to make changes to existing web login pages.

➔ Onboard device provisioning pages are now managed from the Web Login tab within provisioning settings

Name	Page Title	Page Name	Page Skin
aruba-test		aruba-test	(Default)
<div>  Edit            Duplicate            Delete            Translations            Launch         </div>			
1 web login  Reload			
Show all rows			

## 6 Demonstration -1

### 6.1 Dot1x Test for updating the Endpoint attribute

Now the client connects to the dot1x service with username staff1

aruba

a Hewlett Packard  
Enterprise company

VIRTUAL  
CONTROLLER

CP-LabVC

Search

2 Networks

+

Name ▾

Clients

Guest-ES

0

Sec-ES

1

1 Access Point

+

Name ▾

Clients

20:4c:03:17:a0:4c \*

1

1 Client

Name ▾

IP Address

ESSID

Access Point

staff1

10.10.21.22

Sec-ES

20:4c:03:17:a0:4c

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

Request Details	
Summary	Input
Date and Time:	Nov 05, 2019 12:29:13 AEDT
End-Host Identifier:	a088b450c084
Username:	staff1
Access Device IP/Port:	10.10.20.10:0 (CP-LabVC / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Aruba 802.1X Wireless
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:wlan-dc.wlan.net
Authorization Source:	[Time Source], Lab-AD1
Roles:	[User Authenticated]
Enforcement Profiles:	aa Aruba 802.1X Wireless Update Endpoint Secure, aa Aruba 802.1X Wireless-Staff
Service Monitor Mode:	Disabled
Online Status:	Online
Showing 1 of 1-14 records	
Change Status Show Configuration Export Show Logs Close	


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

Dashboard	Configuration » Identity » Endpoints	Dashboard	Configuration » Identity » Endpoints
Monitoring	Endpoint	Monitoring	Endpoint
Configuration	Attributes	Configuration	Attributes
Service Templates & Wizards	Policy Cache	Service Templates & Wizards	Policy Cache
Services	MAC Address a088b450c084	Services	Attribute Value
Authentication	Description	Authentication	1. secure = true
Methods	Status	Methods	2. Click to add...
Sources	Known client	Sources	
Single Sign-On (SSO)	Unknown client	Single Sign-On (SSO)	
Local Users	Disabled client	Local Users	
Endpoints	MAC Vendor Intel Corporate	Endpoints	
Static Host Lists	Added by Policy Manager	Static Host Lists	
Roles	Online Status Online	Roles	
Role Mappings	Connection Type Wireless	Role Mappings	
Posture	Access Point 204c0317a04c	Posture	
Posture Policies	Network SSID Sec-ES	Posture Policies	
Audit Servers		Audit Servers	
Enforcement		Enforcement	
Policies		Policies	
Profiles		Profiles	
Network		Network	
Devices		Devices	
Device Groups		Device Groups	

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.

  
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.



ClearPass Guest

Please login to the network using your username and password.


Login	
Username:	<input type="text" value="cp@aa.com"/>
Password:	<input type="password" value="*****"/>
<input type="button" value="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
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
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"

  
an 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)

Request Details	
Summary	Input
Login Status:	REJECT
Session Identifier:	R00000012-01-5dc0dd07
Date and Time:	Nov 05, 2019 13:23:03 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]
Enforcement Profiles:	[Deny Access Profile]
Service Monitor Mode:	Disabled
Showing 1 of 1-24 records <a href="#">Show Configuration</a> <a href="#">Export</a> <a href="#">Show Logs</a> <a href="#">Close</a>	

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.

Summary	Input	Output	Alerts
Username:	cp@aa.com		
End-Host Identifier:	a088b450c084 (Computer / Windows / Windows)		
Access Device IP/Port:	10.10.20.10:0 (CP-LabVC / Aruba)		
RADIUS Request			
Authorization Attributes			
Computed Attributes			
Authentication:ErrorCode	0		
Authentication:Full-Username	cp@aa.com		
Authentication:Full-Username-Normalized	cp@aa.com		
Authentication:MacAuth	NotApplicable		
Authentication:OuterMethod	PAP		
Authentication:Posture	Unknown		
Authentication:Source	[Guest User Repository]		
Authentication:Status	User		
Showing 1 of 1-24 records <a href="#">Show Configuration</a> <a href="#">Export</a> <a href="#">Show Logs</a> <a href="#">Close</a>			

Summary	Input	Output	Alerts
Endpoint:secure	true		
GuestUser:Company Name	cpuser		
GuestUser:Create Time	2019-11-05T01:44:22+00:00		
GuestUser:do_expire	1		
GuestUser:Email	cp@aa.com		
GuestUser:expired_notify_status	1		
GuestUser:expire_postlogin	0		
GuestUser:remote_addr	192.168.1.126		
GuestUser:Role ID	2		
GuestUser:simultaneous_use	5		
GuestUser:source	create_user		
GuestUser:sponsor_profile_name	Super Administrator		
GuestUser:Visitor Name	cpuser		

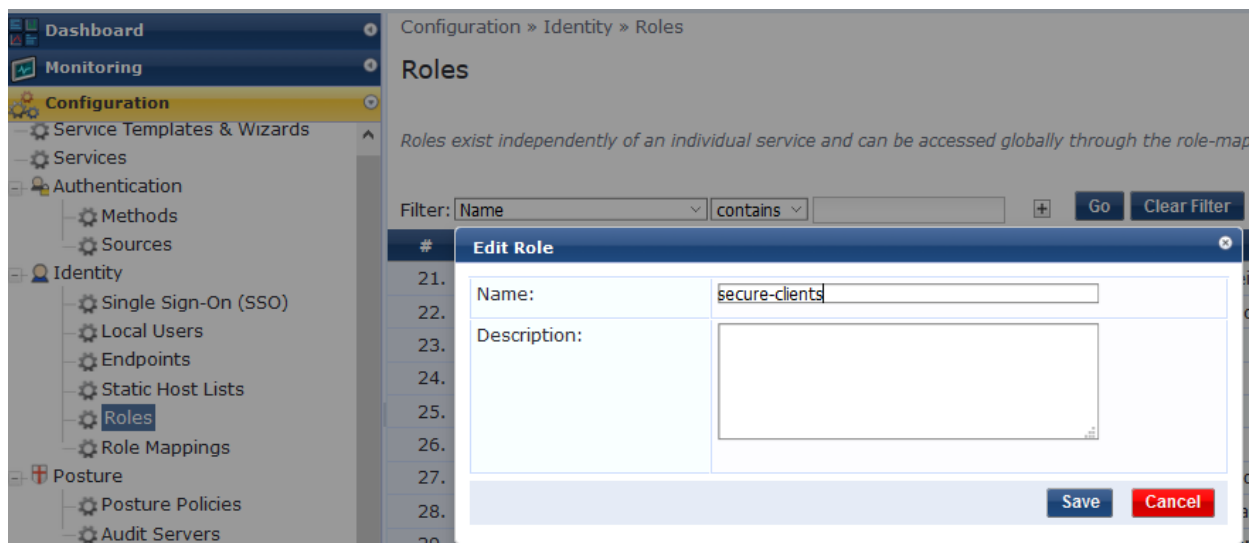
And looking at the Instant AP, we see that the second cp@aa.com “guest” user is stuck in pre-auth user role.

aruba a Hewlett Packard Enterprise company VIRTUAL CONTROLLER CP-LabVC								
2 Clients								
Name	IP Address	MAC address	OS	ESSID	Access Point	Channel	Type	Role
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	149+	AN	Guest-ES

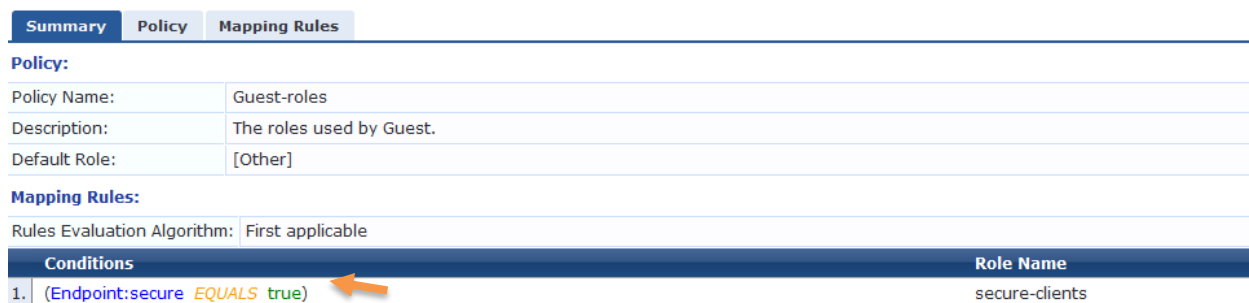
## 7 Demonstration -2

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"



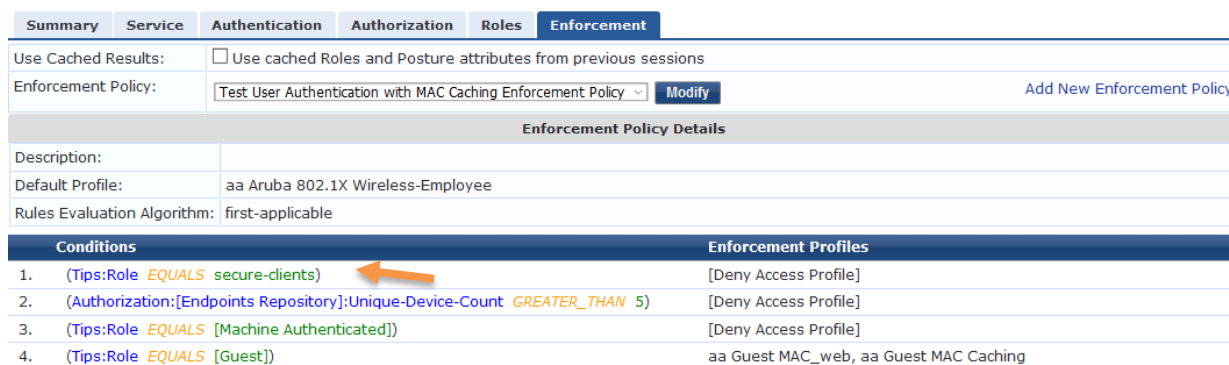
Then we'll create a new role mapping policy.



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



Finally modifying our enforcement policy to use Tips:role .



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.

<div>aruba a Hewlett Packard Enterprise company</div> <div>VIRTUAL CONTROLLER</div> <div>CP-LabVC</div>									
2 Clients									
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	