

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

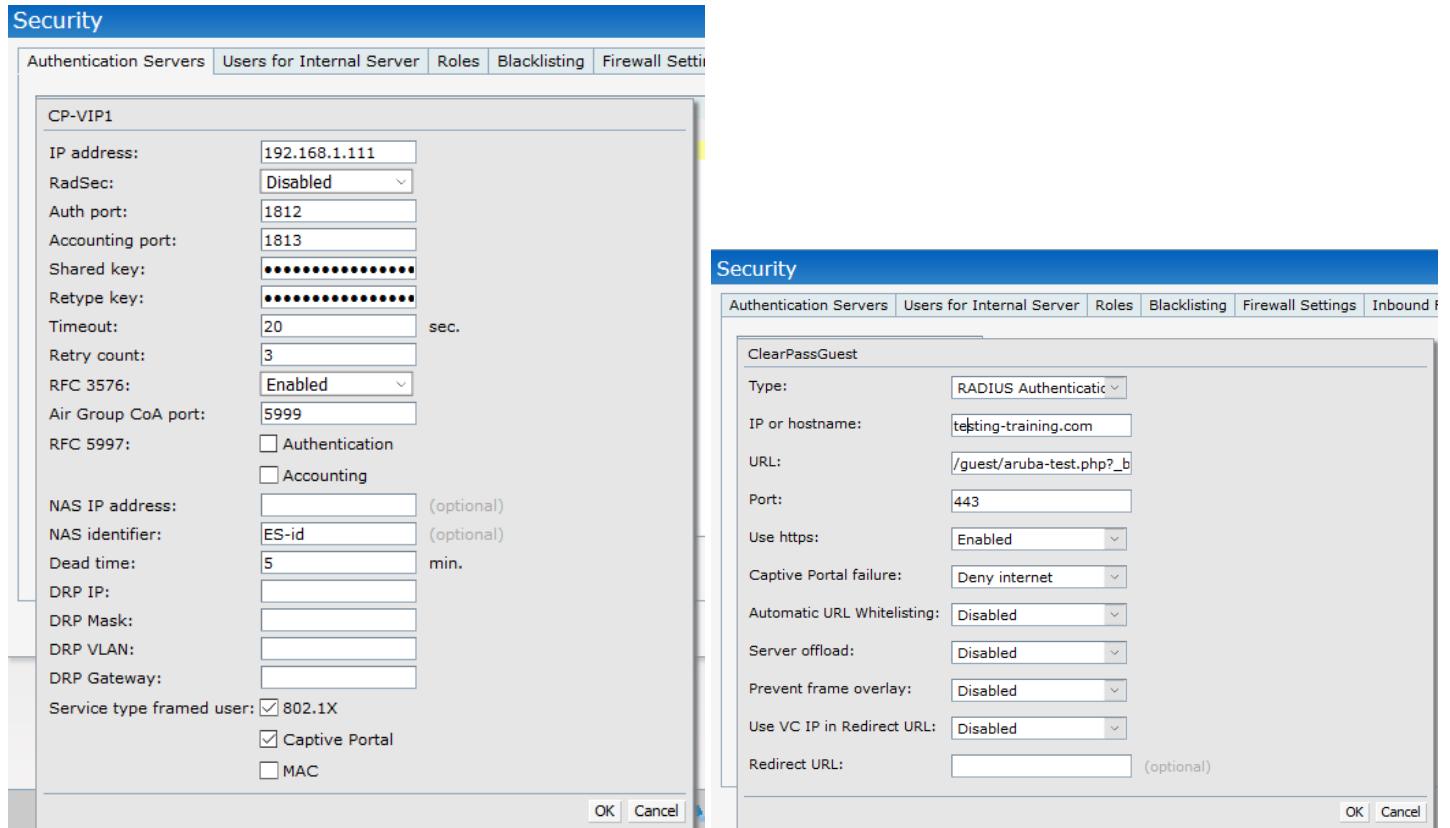
- Aruba Instant version 8.3. or later
- ClearPass 6.7 or later
- A Layer three switch

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.

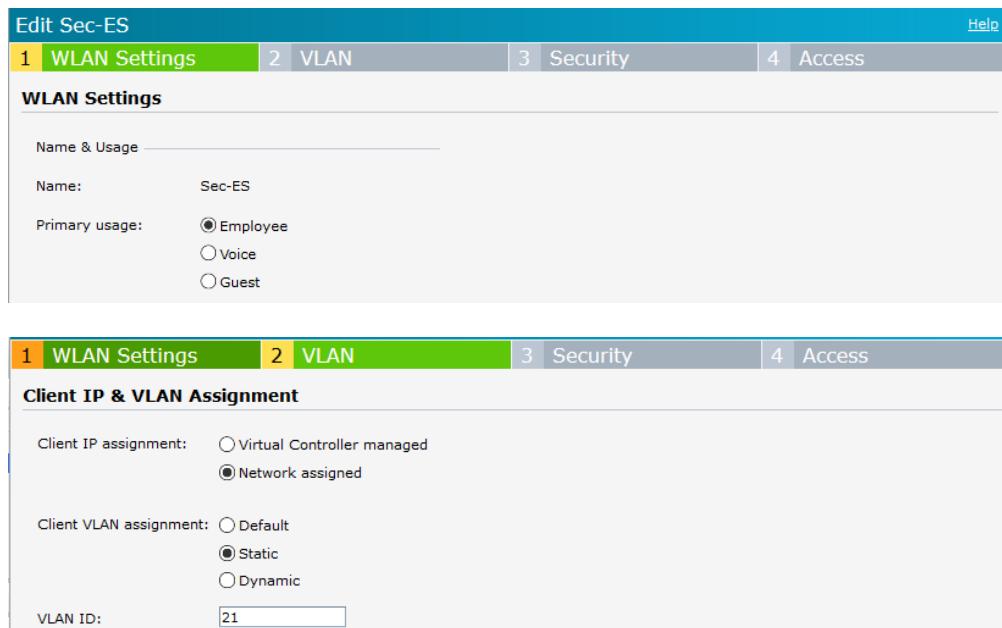
3.1 Authentication Server and Captive Portal Profile Configuration

First we'll configure the RADIUS server.



3.2 Dot1x WLAN Configuration

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



Security Level

More Secure	Key management: <input type="text" value="WPA-2 Enterprise"/>
Enterprise	Authentication server 1: <input type="text" value="CP-VIP1"/> <input type="button" value="Edit"/>
Personal	Authentication server 2: <input type="text" value="-- Select Server --"/>
Open	EAP offload: <input type="text" value="Disabled"/>
Less Secure	Reauth interval: <input type="text" value="0"/> hrs.
	Authentication survivability: <input type="text" value="Disabled"/>
	MAC authentication: <input type="checkbox"/> Perform MAC authentication before 802.1X
	<input type="checkbox"/> MAC authentication fail-thru
	Accounting: <input type="text" value="Use authentication servers"/>
	Accounting interval: <input type="text" value="1"/> min.
	Blacklisting: <input type="text" value="Disabled"/>
	Enforce DHCP: <input type="text" value="Disabled"/>
Fast Roaming	
	Opportunistic Key Caching(OKC): <input type="checkbox"/>
	802.11r: <input type="checkbox"/>
	802.11k: <input type="checkbox"/>
	802.11v: <input type="checkbox"/>

Access Rules

More Control	
- Role-based	
- Network-based	
Unrestricted	No restrictions on access based on destination or type of traffic
Less Control	

3.3 Guest WLAN Configuration

WLAN Settings

Name & Usage	
Name:	Guest-ES
Primary usage:	<input type="radio"/> Employee <input type="radio"/> Voice <input checked="" type="radio"/> Guest

Client IP & VLAN Assignment

Client IP assignment:	<input type="radio"/> Virtual Controller managed <input checked="" type="radio"/> Network assigned
Client VLAN assignment:	<input type="radio"/> Default <input checked="" type="radio"/> Static <input type="radio"/> Dynamic
VLAN ID:	<input type="text" value="22"/>

Security Level

Splash page type:

Captive portal proxy server:

Captive portal profile:

WISPr:

MAC authentication:

Auth server 1:

Auth server 2:

Reauth interval: hrs.

Accounting:

Accounting mode:

Accounting interval: min.

Blacklisting:

Enforce DHCP:

Disable if uplink type is: 3G/4G Wifi Ethernet

Encryption:

Access Rules

More Control

- Role-based
- Network-based
- Unrestricted

Less Control

Roles

Guest-ES
default_wired_port_profile
wired-SetMeUp

Access Rules

Role Assignment Rules

Default role: Guest-ES

Assign pre-authentication role:

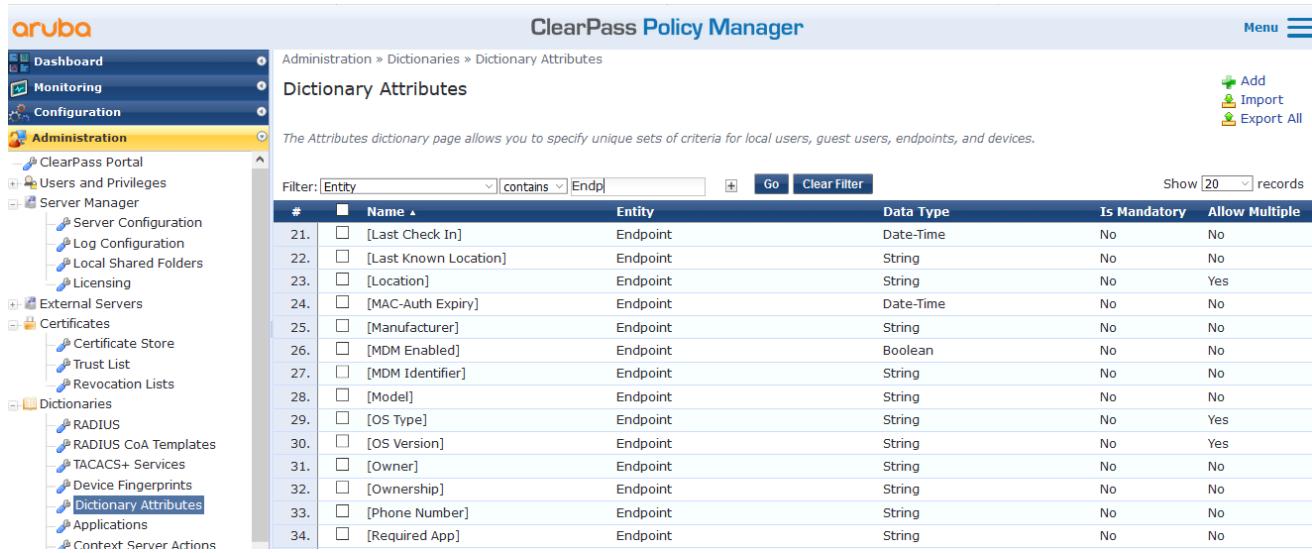
4 ClearPass dot1x Service Configuration

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".



Entity	Endpoint
Name	secure
Data Type	Boolean
Is Mandatory	<input type="radio"/> Yes <input checked="" type="radio"/> No
Default Value (optional)	<input type="radio"/> True <input type="radio"/> False (e.g., true / false)

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:	<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		
Service Rule			
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	
Click to add...			

Summary	Service	Authentication	Roles	Enforcement
<p>Authentication Methods:</p> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> [EAP MSCHAPv2] [EAP PEAP Without Fast Reconnect] [EAP TLS] </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> Move Up ↑ Move Down ↓ </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Remove View Details Modify </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;"> -Select to Add- </div>				
Add New Authentication Method				
<p>Authentication Sources:</p> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Lab-AD1 [Active Directory] [Local User Repository] [Local SQL DB] </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> Move Up ↑ Move Down ↓ </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Remove View Details Modify </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;"> -Select to Add- </div>				
Add New Authentication Source				
<p>Strip Username Rules:</p> <input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes				
<p>Service Certificate:</p> <div style="border: 1px solid #ccc; padding: 2px;"> -Select to Add- </div> <div style="text-align: right; margin-top: 5px;"> View Certificate Details </div>				

Summary	Service	Authentication	Roles	Enforcement															
<p>Role Mapping Policy:</p> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px;"> -Select- </div> <div style="margin: 0 10px;"> Modify </div> <div style="text-align: right;"> Add New Role Mapping Policy </div> </div>																			
Role Mapping Policy Details																			
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>Description:</td> <td colspan="4">-</td> </tr> <tr> <td>Default Role:</td> <td colspan="4">-</td> </tr> <tr> <td>Rules Evaluation Algorithm:</td> <td colspan="4">-</td> </tr> </table>					Description:	-				Default Role:	-				Rules Evaluation Algorithm:	-			
Description:	-																		
Default Role:	-																		
Rules Evaluation Algorithm:	-																		
Conditions																			
Role																			
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Conditions</th> <th>Role</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	Role	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	Role																		
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															
<p>Use Cached Results:</p> <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions																			
<p>Enforcement Policy:</p> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px;"> aa Aruba 802.1X Wireless Enforcement Policy </div> <div style="margin: 0 10px;"> Modify </div> <div style="text-align: right;"> Add New Enforcement Policy </div> </div>																			
Enforcement Policy Details																			
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>Description:</td> <td colspan="4"></td> </tr> <tr> <td>Default Profile:</td> <td colspan="4">[Deny Access Profile]</td> </tr> <tr> <td>Rules Evaluation Algorithm:</td> <td colspan="4">first-applicable</td> </tr> </table>					Description:					Default Profile:	[Deny Access Profile]				Rules Evaluation Algorithm:	first-applicable			
Description:																			
Default Profile:	[Deny Access Profile]																		
Rules Evaluation Algorithm:	first-applicable																		
Conditions																			
Enforcement Profiles																			
<table border="1" style="width: 100%; border-collapse: collapse;"> <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>1. 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>					1. (Authorization:Lab-AD1:memberOf CONTAINS stud)	aa Aruba 802.1X Wireless-Student, aa Aruba 802.1X Wireless Update Endpoint Secure	1. 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									
1. (Authorization:Lab-AD1:memberOf CONTAINS stud)	aa Aruba 802.1X Wireless-Student, aa Aruba 802.1X Wireless Update Endpoint Secure																		
1. 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
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:	<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	<input type="button" value="Edit"/> <input type="button" value="Delete"/>		
2. Connection	Client-Mac-Address	NOT_EQUALS	<input type="button" value="Edit"/> <input type="button" value="Delete"/>		
3. Radius:Aruba	Aruba-Essid-Name	CONTAINS	<input type="button" value="Edit"/> <input type="button" value="Delete"/>		
4. Click to add...					

Summary Service **Authentication** Authorization Roles Enforcement

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

Summary Service **Authentication** Authorization Roles Enforcement

Authorization Details:	<p>Authorization sources from which role mapping attributes are fetched (for each Authentication Source)</p> <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> <p>Additional authorization sources from which to fetch role-mapping attributes -</p> <p>[Endpoints Repository] [Local SQL DB] <input type="button" value="Remove"/> [Time Source] [Local SQL DB] <input type="button" value="View Details"/> <input type="button" value="Modify"/></p> <p>-Select to Add-</p>			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]	Add New Authentication Source
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]									

Summary Service **Authentication** Authorization Roles **Enforcement**

Role Mapping Policy:	<p>[Guest Roles] <input type="button" value="Modify"/></p>	Add New Role Mapping Policy														
<p>Role Mapping Policy Details</p> <table border="1"> <tr> <td>Description:</td> <td>The roles used by Guest.</td> </tr> <tr> <td>Default Role:</td> <td>[Employee]</td> </tr> <tr> <td>Rules Evaluation Algorithm:</td> <td>first-applicable</td> </tr> <tr> <td>Conditions</td> <td>Role</td> </tr> <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> </table>			Description:	The roles used by Guest.	Default Role:	[Employee]	Rules Evaluation Algorithm:	first-applicable	Conditions	Role	1. (GuestUser:Role ID EQUALS 1)	[Contractor]	2. (GuestUser:Role ID EQUALS 2)	[Guest]	3. (GuestUser:Role ID EQUALS 3)	[Employee]
Description:	The roles used by Guest.															
Default Role:	[Employee]															
Rules Evaluation Algorithm:	first-applicable															
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:	<p>[Test User Authentication with MAC Caching Enforcement Policy] <input type="button" value="Modify"/></p>	Add New Enforcement Policy																
<p>Enforcement Policy Details</p> <table border="1"> <tr> <td>Description:</td> <td></td> </tr> <tr> <td>Default Profile:</td> <td>[Deny Access Profile]</td> </tr> <tr> <td>Rules Evaluation Algorithm:</td> <td>first-applicable</td> </tr> <tr> <td>Conditions</td> <td>Enforcement Profiles</td> </tr> <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> </table>			Description:		Default Profile:	[Deny Access Profile]	Rules Evaluation Algorithm:	first-applicable	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
Description:																		
Default Profile:	[Deny Access Profile]																	
Rules Evaluation Algorithm:	first-applicable																	
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 visitors.

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

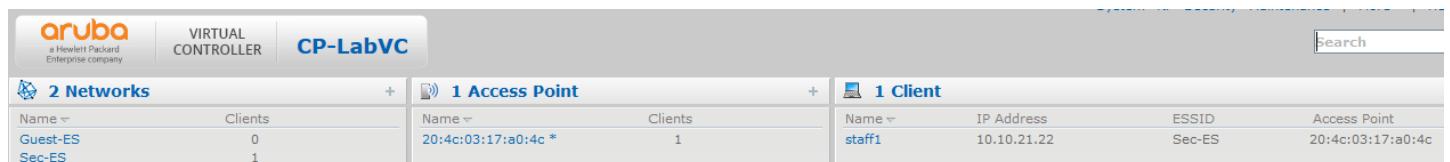
Onboard device provisioning pages are now managed from the Web Login tab within provisioning settings

△ Name	Page Title	Page Name	Page Skin
aruba-test		aruba-test	(Default)
<input type="button" value="Edit"/> <input type="button" value="Duplicate"/> <input type="button" value="Delete"/> <input type="button" value="Translations"/> <input type="button" value="Launch"/>			
1 web login	<input type="button" value="Reload"/>		<input type="button" value="Show all rows"/>

6 Demonstration -1

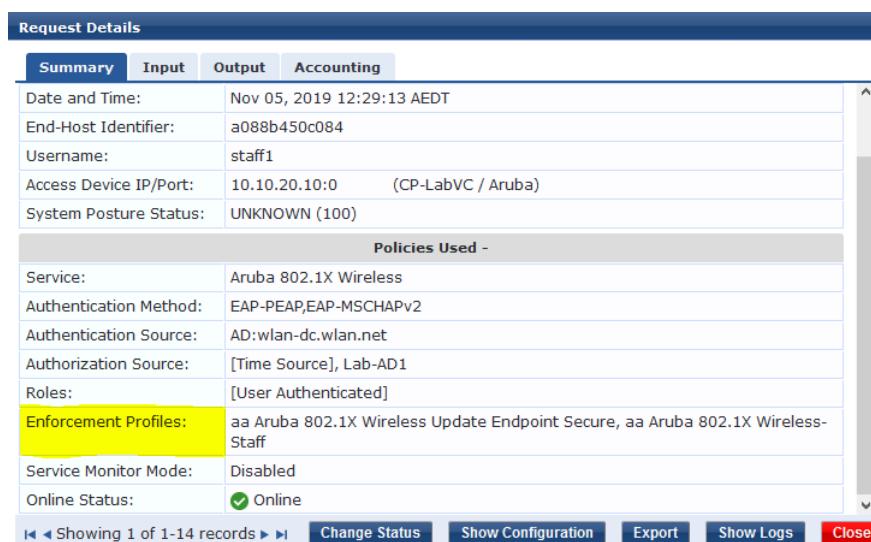
6.1 Dot1x Test for updating the Endpoint attribute

Now the client connects to the dot1x service with username staff1



The screenshot shows the Aruba Virtual Controller interface with three main sections: '2 Networks' (Guest-ES, Sec-ES), '1 Access Point' (20:4c:03:17:a0:4c *), and '1 Client' (staff1, IP Address: 10.10.21.22, ESSID: Sec-ES, Access Point: 20:4c:03:17:a0:4c). A search bar is at the top right.

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



The screenshot shows the 'Request Details' page with tabs for Summary, Input, Output, and Accounting. The Summary tab displays the following details:

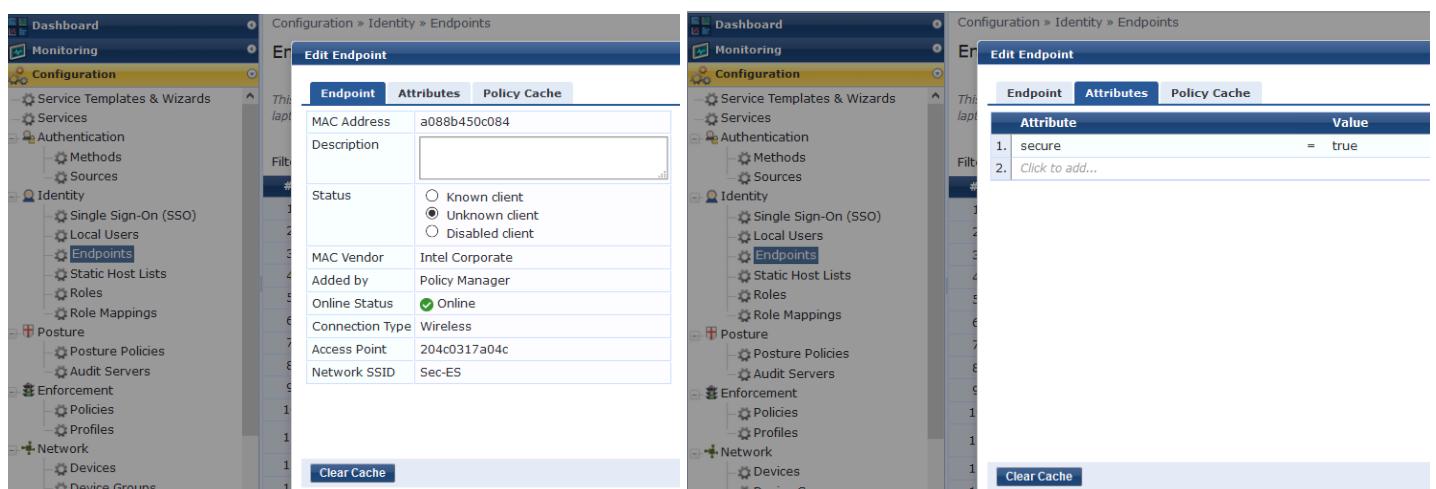
Date and Time:	Nov 05, 2019 12:29:13 AEDT
End-Host Identifier:	a088b450c084
Username:	staff1
Access Device IP/Port:	10.10.20.10:0 (CP-LabVC / Aruba)
System Posture Status:	UNKNOWN (100)

The 'Policies Used' section shows:

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

At the bottom are buttons for 'Change Status', 'Show Configuration', 'Export', 'Show Logs', and 'Close'.

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



The screenshot shows the 'Edit Endpoint' screen for an endpoint with MAC Address a088b450c084. The 'Attributes' tab is selected, showing the 'secure' attribute set to true.

Attribute	Value
secure	= true
Click to add...	

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.

CP-LabVC								
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

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



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"

CP-LabVC								
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)

Request Details

Summary	Input	Output	Alerts
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 ▶ Show Configuration Export Show Logs Close

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 ▶ Show Configuration Export Show Logs Close

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.

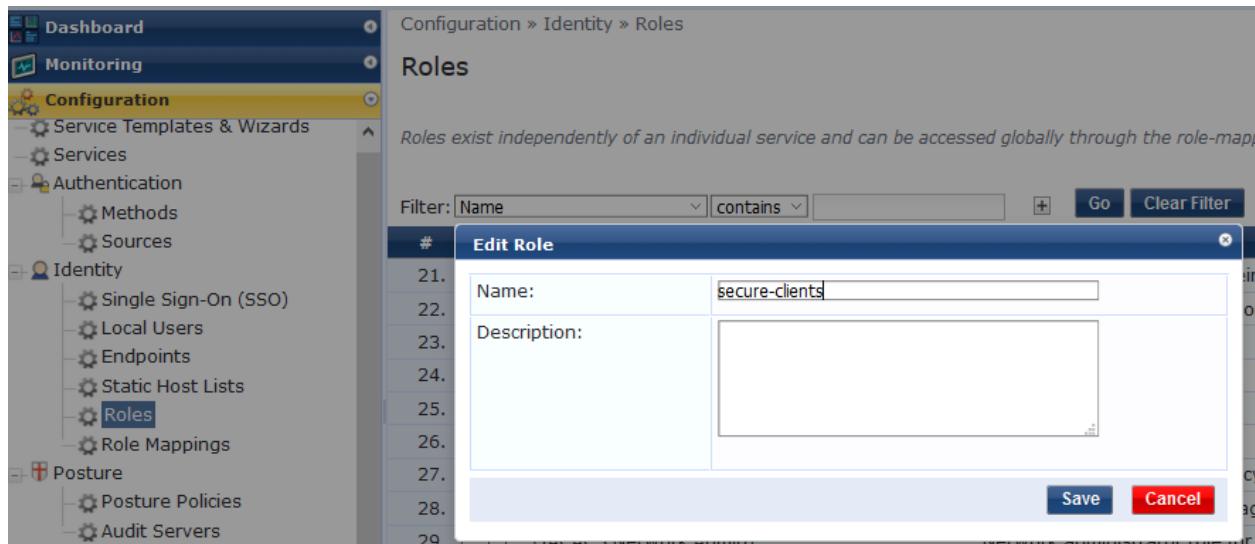
aruba a Hewlett Packard Enterprise company VIRTUAL CONTROLLER CP-LabVC

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

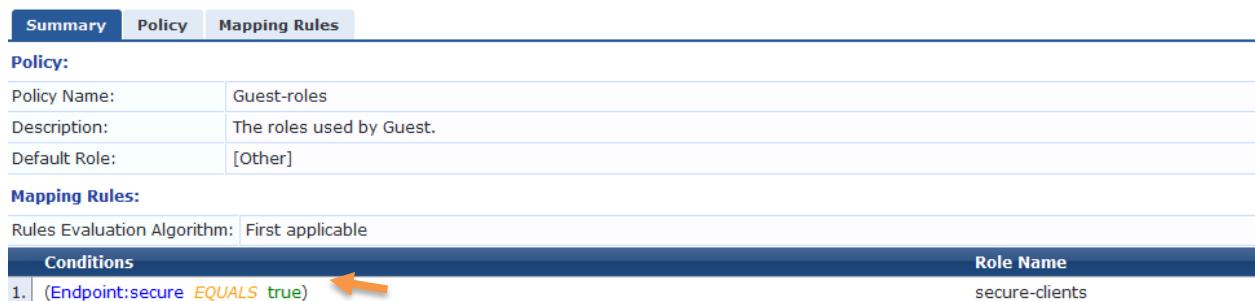
7 Demonstration -2

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"



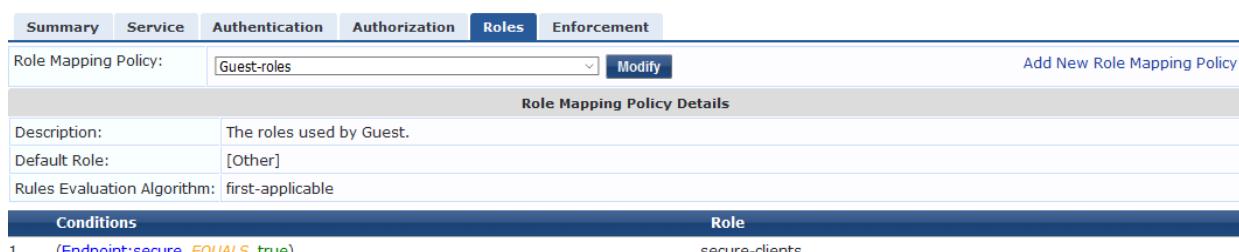
The screenshot shows the Aruba Configuration interface. The left sidebar is titled 'Configuration' and includes 'Service Templates & Wizards', 'Services', 'Authentication' (with 'Methods' and 'Sources' sub-options), 'Identity' (with 'Single Sign-On (SSO)', 'Local Users', 'Endpoints', 'Static Host Lists', 'Roles' (selected), and 'Role Mappings'), 'Posture' (with 'Posture Policies' and 'Audit Servers'). The main panel is titled 'Configuration > Identity > Roles' and shows a table titled 'Edit Role'. The table has a single row with the following data: # 21, Name: 'secure-clients', and Description: (empty). There are 'Save' and 'Cancel' buttons at the bottom. A filter bar at the top allows searching by 'Name'.

Then we'll create a new role mapping policy.



The screenshot shows the Aruba Configuration interface. The top navigation bar has tabs: 'Summary' (selected), 'Policy', and 'Mapping Rules'. The 'Policy' tab is active. The main panel shows a table for 'Guest-roles' with one condition: '1. (Endpoint:secure EQUALS true)'. An orange arrow points to this condition. The 'Conditions' column has a blue link '(Endpoint:secure EQUALS true)'. The 'Role Name' column has the value 'secure-clients'.

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



The screenshot shows the Aruba Configuration interface. The top navigation bar has tabs: 'Summary', 'Service', 'Authentication', 'Authorization', 'Roles' (selected), and 'Enforcement'. The 'Roles' tab is active. The main panel shows a table for 'Guest-roles' with one condition: '1. (Endpoint:secure EQUALS true)'. An orange arrow points to this condition. The 'Conditions' column has a blue link '(Endpoint:secure EQUALS true)'. The 'Role' column has the value 'secure-clients'.

Finally modifying our enforcement policy to use Tips:role .



The screenshot shows the Aruba Configuration interface. The top navigation bar has tabs: 'Summary', 'Service', 'Authentication', 'Authorization', 'Roles', and 'Enforcement' (selected). The 'Enforcement' tab is active. The main panel shows a table for 'Test User Authentication with MAC Caching Enforcement Policy' with four conditions: 1. (Tips:Role EQUALS secure-clients), 2. (Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 5), 3. (Tips:Role EQUALS [Machine Authenticated]), and 4. (Tips:Role EQUALS [Guest]). An orange arrow points to the first condition. The 'Conditions' column has blue links for each condition. The 'Enforcement Profiles' column lists '[Deny Access Profile]' for the first three conditions and 'aa Guest MAC_web, aa Guest MAC Caching' for the fourth condition.

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.

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	149E	AN	Guest-ES			