# Contents

	1.1	Revision History	1
		ted AD group Configuration – Method1	
	2.1	Active Directory Groups	2
	2.2	ClearPass Configuration	3
	2.3	Testing	7
	2.4	Modifying Enforcement policy	8
3	Nes	ted AD group Configuration – Method2	.11
	3.1	ClearPass Configuration	.11
	3.2	Testing	.12

# **1.1** Revision History

DATE	VERSION	EDITOR	CHANGES
02 Apr 2021	0.1	Ariya Parsamanesh	Initial creation
18 Apr 2021	0.2	Ariya Parsamanesh	Added the second method

# **2 Nested AD group Configuration – Method1**

Here we are going create a ClearPass enforcement policy to check if the user is member of nested or higher level AD group. There are many cases that the users are member of a sub group that are all part of a higherlevel group and you want to create a enforcement policy with fewer rules to check for the membership of a AD user group.

## 2.1 Active Directory Groups

Here are our current AD groups, the user called "test1" being a member of "test-users" group which is the member of "all-test-users" group.

Windows Server 2008			Windows Server 2008	
test 1 Properties	4		test-users Properties	
Security Environment Sessions Remote control				
Terminal Services Profile COM+ Attribute Editor	🛛 😤 😣 🕯	ê 7	Object Security Attribute Editor	
General         Address         Account         Profile         Telephones         Organization           Published Certificates         Member Of         Password Replication         Dial-in         Object		Typ Use		🔧 📚 🗎
Member of:		Sec	Sec Member of:	
Name Active Directory Domain Services Folder	ily Domain	. Sec Use	Name Active Directory Domain Services Folder	
Domain Users wlan.net/Users		Sec	all-test-users wlan.net/Users	
test-users wlan.net/Users	pr Owners	Sec	Sec Contraction of the second s	only Domain
		Use		1
		Use Use		:
	ers	Sec		tor Owners
	Controllers	Sec		1
		Use	Jse	1
		Sec		1
Add Remove		Sec		vers
		Sec Use		n Controllers
		Use	J9C	
Primary group: Domain Users		Sec		
There is no need to change Primary group unless		Use		
you have Macintosh clients or POSIX-compliant		Use		
applications.		Use	Ise in the Global Catalog, such as universal groups.	
		Sec		1

Windows S	Windows Server 2008						
all-test-users P	roperties		?	×			
Object	Secu		Attribute Editor	į 🗌			
General	Members	Member Of	Managed By				
Members:							
Name		ctory Domain Service	es Folder				
& test-user	s wlan.net/U	sers		ass			
				IE -			
				assv			
				ators			
				Ц.			
				ers			
				rs			
				н.			
Add	Remove			s			
Add	nemove			only			

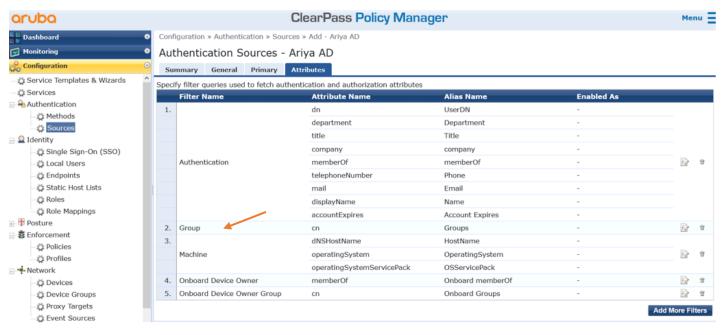
ClearPass can check if the test1 is memberof "test-users" but the condition will fail for checking memberof "all-testusers" group. So, the aim here is to be able to check if the user is in a sub-group under "all-test-users" group.

# 2.2 ClearPass Configuration

We are assuming you already have joined ClearPass to the AD domain and have configured an Authentication source for it as seen below.

arv	JÞA		ClearPass Policy Manager			
Da	ashboard O	Configuration » Authentication » Sources » Add - Ariya AD				
💽 Ma	onitoring O	Authentication Sources - Ariya AD				
🖧 Co	onfiguration 💿	Summary General	Primary Attributes			
—;;; S	Service Templates & Wizards	General:				
—Q S	Services	General:				
⊡- <del>2</del> A	uthentication	Name:	Ariya AD			
	– 🛱 Methods	Description:				
	-🛱 Sources	Type:	AD			
🚨 I	dentity	Use for Authorization:	Enabled			
	– 🛱 Single Sign-On (SSO)	Authorization Sources:	-			
	- C Local Users					
	– 😋 Endpoints	Primary:				
	– 🗘 Static Host Lists	Hostname:	192.168.1.250			
	- 🗘 Roles	Connection Security:	None			
	Role Mappings	Port:	389			
🛨 🕇 Þ	osture	Verify Server Certificate:	true			
💈 E	nforcement	Bind DN:	administrator@wlan.net			
	– 🛱 Policies	Bind Password:	*****			
	– 🛱 Profiles	NetBIOS Domain Name:	WLAN			
<b></b> - N	letwork	Base DN:	dc=wlan,dc=net			
	- 🗘 Devices		SubTree Search			
	- Device Groups	Search Scope:				
	– 🗘 Proxy Targets	LDAP Referrals:	false			
	– 🛱 Event Sources	Bind User:	true			
—.;;; N	letwork Scan	User Certificate:	userCertificate			

Now checking the attributes that were created by default when you configured the authentication source.



We need to modify and add couple of attributes to the authentication source. The first step is to rename the filter named "Groups". Change the Filter Name to "SubGroup" and the Alias Name to "SubGroup".

Сог	Configure Filter								
	Configuration Attribute	es Browse Filter							
Filter Name: SubGroup									
Fil	lter Query:	(distinguishedName=%{memberOf})							
	Name	Alias Name	Data type	Enabled As					
1.	cn	SubGroups	String	- 1	Ì				
2.	memberOf	SubGroupmemberOf	String 💌	🗆 Role 🔲 🛄 🛍	Ì				
3.	Click to add								



Then add/modify attributes to look like what is shown above. The name must be "memberOf" (it is case sensitive) and the Alias Name should be "SubGroupmemberOf". So, when you save it, this is what you should get.

Aut	hentication Sources - Ariy	a AD				
Su	nmary General Primary Attri	butes				
Speci	fy filter queries used to fetch authentic	ation and authorization attributes				
	Filter Name	Attribute Name	Alias Name	Enabled As		
1.		dn	UserDN	-		
		department	Department	-		
		title	Title	-		
		company	company	-		
	Authentication	ation memberOf memberOf -		-	₽ <sup>2</sup>	Ť
		telephoneNumber	Phone -			
		mail	Email	-		
		displayName	Name	-		
		accountExpires	Account Expires	-		
2.		cn	SubGroups	-	E.	Ť
	SubGroup	memberOf	SubGroupmemberOf	-	1	
3.		dNSHostName	HostName	-		
	Machine	operatingSystem	OperatingSystem	-	Ð	Ť
		operatingSystemServicePack	OSServicePack	-		
4.	Onboard Device Owner	memberOf	Onboard memberOf	-	Ð	Ť
5.	Onboard Device Owner Group	cn	Onboard Groups	-	Ð	Û
3. 4.	SubGroup Machine Onboard Device Owner	telephoneNumber mail displayName accountExpires cn memberOf dNSHostName operatingSystem operatingSystemServicePack memberOf	Phone Email Name Account Expires SubGroups SubGroupmemberOf HostName OperatingSystem OSServicePack Onboard memberOf	- - - - - - - - - - - - - - - - - - -	Þ	•

Now, we'll add another filter by clicking the "Add More Filters" button on the bottom right corner of the window. Click the "Configuration" tab on the next window and enter "OneLevelUp" as the Filter Name. In the Filter Query box, enter "(distinguishedName=%{SubGroupmemberOf})".

This tells the filter to search for the variable called SubGroupmemberOf, which was set in the initial query of the user record.

Conf	Configure Filter								
C	onfiguration Attribut	es Browse Filter							
Filter Name: OneLevelUp									
Filter Query:		(distinguishedName=%{SubG	roupmemberOf})		.d				
	Name	Alias Name	Data type	Enabled As					
1.	cn	OneLevelUp	String	-	Ť				
2.	memberOf	OneLevelUpmemberOf	String	-	Ť				
з.	Click to add								

Then add the two entries as "cn" and "memberOf" as shown above. Once it is saved, you should see the following as the final attributes that are now defined for the AD authentication source.

Authentication Sources - Ariya AD

nmary General Primary Attribute
---------------------------------

Filter Name	Attribute Name	Alias Name	Enabled As		
1.	dn	UserDN	-		
	department	Department	-		
	title	Title	-		
	company	company	-		
Authentication	memberOf	memberOf -		E)	)
	telephoneNumber	Phone	-		
	mail	Email	-		
	displayName	Name	-		
	accountExpires	Account Expires	-		
2. SubGroup	cn	SubGroups	-	Ð	) iii
SubGroup	memberOf	SubGroupmemberOf	-	1.0	, m
3.	dNSHostName	HostName	-		
Machine	operatingSystem	OperatingSystem	-	Ð	) 1
	operatingSystemServicePack	OSServicePack	-		
4. Onboard Device Owner	memberOf	Onboard memberOf	-	Ð	1
5. Onboard Device Owner Grou	ıp cn	Onboard Groups	-	E)	) D
6. OneLevelUp	cn	OneLevelUp	-	Đ	) iii
Oneceverop	memberOf	OneLevelUpmemberOf	-	19	

Now for ClearPass policies to use these new attributes, we need Role Mapping to map the attributes to a TIPS role that then gets referenced in the enforcement policy. First create a Role called "all-test-group-member"

aruba		ClearPass Policy Manager				
Dashboard	Configuration	n » Identity » Roles				
Monitoring	Roles					
Configuration	Θ					
<ul> <li>Service Templates &amp; Wizards</li> <li>Services</li> </ul>	Roles exist il	ndependently of an	individual service and ca	an be accessed globall	ly through the role-mapping po	
	Filter: Name		v contains v	+	Go Clear Filter	
Methods     Sources	#	Name 🔺		Description		
🖃 🚨 Identity	Edit Role				🔊 version 1 requ	
<ul> <li>Single Sign-On (SSO)</li> <li>Local Users</li> </ul>	Role ID:		3006		version 2 requ	
- C Endpoints	Name:		all-test-group-member		ess to Aruba d	
- Carlie Host Lists	Descript	ion:			Aruba device	
Roles					view and ma	
— Role Mappings						
관 📅 Posture 🖃 💐 Enforcement					self-provisior	
				Save	Cancel	
- 🛱 Profiles		[Guet]		Detault role to	ar a Guest	

Then go to Role Mappings and map that role to Authorisation condition as shown below.

aruba		ClearPass Policy Manager				
Dashboard O	Configuration » Identity » I	Configuration » Identity » Role Mappings » Edit - nested-group				
🖼 Monitoring 🔹 🔍	Role Mappings - n	ested-group				
🖧 Configuration 📀	Summary Policy Ma	apping Rules				
<ul> <li>Service Templates &amp; Wizards</li> <li>Services</li> </ul>	Policy:					
- Authentication	Policy Name:	nested-group				
- 🛱 Methods	Description:					
- 🛱 Sources	Default Role:	all-test-group-member				
∃	Mapping Rules:					
– C Local Users	Rules Evaluation Algorithm	: First applicable				
- C Endpoints	Conditions		Role Name			
– 🗘 Static Host Lists	1. (Authorization:Ariya Al	D:UpOneLevelmemberOf CONTAINS all-test-users)	all-test-group-member			
- 🛱 Roles						
- 🔅 Role Mappings						

aruba	ClearPass Policy Manager					
Dashboard O	Configuration » Identity » R	ole Mappings » Edit - nested-group				
🐼 Monitoring 🔹 💿	Role Mappings - nested-group					
🖧 Configuration 📀	Summary Policy Mapping Rules					
<ul> <li>         —</li></ul>	Policy:					
	Policy Name:	nested-group				
- 🗘 Methods	Description:					
- 🛱 Sources	Default Role:	all-test-group-member				
🖃 🚨 Identity	Mapping Rules:					
-‡ Single Sign-On (SSO) -‡ Local Users	Rules Evaluation Algorithm:	First applicable				
- C Endpoints	Conditions		Role Name			
- 🛱 Static Host Lists	1. (Authorization: Ariya AD	:OneLevelUpmemberOf CONTAINS all-test-users)	all-test-group-member			
- 🛱 Roles						
-🎝 Role Mappings						

Now we'll add this role mapping to our existing dot1x service. Here we are showing the whole dot1x service for completeness.

Services - AA Aruba 802.1X Wireless

Summary Service	Authentication Roles Enforcement							
Name:	: AA Aruba 802.1X Wireless							
Description: To authenticate users to an Aruba wireless network via 802.1X.								
Туре:	Aruba 802.1X Wireless							
Status:	Enabled							
Monitor Mode:	$\Box$ Enable to monitor network access without e	nitor network access without enforcement						
More Options:	□ Authorization □ Posture Compliance □ A	Posture Compliance 🛛 Audit End-hosts 🗋 Profile Endpoints 🗆 Accounting Proxy						
		Service Rule						
Matches 🔿 ANY or 🖲	ALL of the following conditions:							
Туре	Name	Operator	Value					
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)		Ť			
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)		Ť			
3. Radius:Aruba	Aruba-Essid-Name	EQUALS	school		Ť			
4. Click to add								

#### Summary Service Authentication Roles Enforcement

Authentication Methods		^		Add New Authentication Method
	[EAP TLS]		Move Up ↑	
			Move Down ↓	
			Remove	
			View Details	
			Modify	
		~		
	Select to Add	~		
Authentication Sources:	Ariya AD [Active Director	d ^		Add New Authentication Source
		-	Move Up ↑	
			Move Down L	
			Remove	
			View Details	
			Modify	
		~		
	Select to Add		~	
Strip Username Rules:	Enable to specify a c	omma-separated I	list of rules to strip	p username prefixes or suffixes
Service Certificate:	Select to Add	~		View Certificate Details
Summary Service	Authentication Roles	Enforcement		
Role Mapping Policy:	nested-group		~ Mod	dify Add New Role Mapping Policy
			Role Mapping Policy	cy Details
Description:				
Default Role:	all-test-group-member	-		
Rules Evaluation Algorit	hm: first-applicable			
Conditions				Role
1. (Authorization: Ariy	/a AD:UpOneLevelmemberC	f CONTAINS all-	test-users)	all-test-group-member

Summa	ry Service	Authentication	Roles	Enforcement					
Use Cach	ed Results:	Use cached	$\Box$ Use cached Roles and Posture attributes from previous sessions						
Enforcem	ent Policy:	AA Aruba 802.	X Wireless	Enforcement Policy	Modify     Add New Enforcement Police				
Enforcement Policy Details									
Descriptio	on:								
Default P	rofile:	AA Aruba 80	AA Aruba 802.1X Wireless Default Profile						
Rules Eva	luation Algor	ithm: first-applicab	le						
Conditions					Enforcement Profiles				
1. <b>(A</b>	uthorization:	norization:Ariya AD:memberOf CONTAINS Staff)			AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint Location				
2. (A	(Authorization:Ariya AD:memberOf CONTAINS Student)			VS Student)	AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireless Update Endpoint Location				
3	(Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Staff)				AA-Aruba 802.1X Wireless Staff Profile, [Update Endpoint Known]				
4. (T A		ALS [Machine Auth zation:Ariya AD:me			AA-Aruba 802.1X Wireless Student Profile, [Update Endpoint Known]				

## 2.3 Testing

We are ready to test our new authorisation role. We have a win10 laptop that is connecting to the dot1x SSID. The username we are using is "test1" which is successfully authenticated. Note the Role that is matched is "all-test-group-member". But the enforcement profile that get used is "AA Aruba 802.1x wireless Default profile"

equest Details					
Summary Input C	Output Accounting				
Login Status:	ACCEPT	'			
Session Identifier:	R0000004-01-60651c8d				
Date and Time:	Apr 01, 2021 12:06:21 AEDT				
End-Host Identifier:	A0-88-B4-50-C0-84				
Username:	test1				
Access Device IP/Port:	192.168.1.57 (MD-1 / Aruba)				
Access Device Name:	7008-1				
System Posture Status:	UNKNOWN (100)				
	Policies Used -				
Service:	AA Aruba 802.1X Wireless				
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2				
Authentication Source:	AD:192.168.1.250				
Authorization Source:	Ariya AD				
Roles:	[User Authenticated], all-test-group-member				
Enforcement Profiles:	AA Aruba 802.1X Wireless Default Profile	•			

Next, we look at the authorisation section, you see the highlight section that corresponds to the attributes we added.

Summary Input	Output	Accounting		
sername:	test1			
nd-Host Identifier:	A0-88-B4-	50-C0-84		
ccess Device IP/Port:	192.168.1	.57	(MD-1 / Aruba)	
RADIUS Request				
Authorization Attribute	es			
Authorization:Ariya A Authorization:Ariya A Authorization:Ariya A	D:Name		CN=test-users,CN=Users,DC=wlan,DC=net test all-test-users	
Authorization:Ariya	AD <mark>:SubGrou</mark>	pmemberOf	CN=all-test-users,CN=Users,DC=wlan,DC=net	
Authorization:Ariya	\D: <mark>SubGrou</mark>	<mark>ps</mark>	test-users	
Authorization: Ariya	D:UserDN		CN=test1,CN=Users,DC=wlan,DC=net	

As you can see from output tab, ClearPass is sending back use-role= employee, because the enforcement policy is matching the "AA Aruba 802.1x wireless Default profile" enforcement profile.

Access Trac	ker Apr	01, 2021 :	10:16:59 AEDT				
Request Detail	s						6
Summary	Input	Output	Accounting				
Enforcement	Profiles:	AA Aruba	a 802.1X Wireless De	efault Profile			
System Postu	ire Status:	UNKNOW	/N (100)				
Audit Posture	Status:	UNKNOW	/N (100)				
RADIUS Res	ponse						Ð
Radius:Arub	ba:Aruba-U	Jser-Role	Employee				
I Showing	1 of 1-5 re	ecords <b>&gt; &gt;</b>	Change Status	Show Configuration	Export	Show Logs	Close

#### 2.4 **Modifying Enforcement policy**

We'll modify the enforcement policy to send back student-user role. We'll click on the dot1x service and then go to enforcement tab and click on "modify"

Services - AA Aruba 802.1X Wireless

	Note: This Service is created by Service Template								
Summary	Service	Authentication	Roles	Enforcement					
Use Cacheo	l Results:	Use cached	Roles an	d Posture attributes from	previous sessions				
Enforceme	nt Policy:	AA Aruba 802.	AA Aruba 802.1X Wireless Enforcement Policy V Modify						
	Enforcement Policy Details								
Description	:								
Default Pro	Default Profile:		AA Aruba 802.1X Wireless Default Profile						
Rules Evalu	ation Algorit	nm: first-applicab	le						
Cond	itions				Enforcement Pro	ofiles			
1. (Aut	horization: Ar	iya AD:memberOf	CONTA	INS Staff)	AA-Aruba 802.1X Update Endpoint L	Wireless Staff Profile, AA Aruba 802.1X Wireless			
2. (Aut	. (Authorization:Ariya AD:memberOf CONTAINS Student)			NS Student)	AA-Aruba 802.1X Update Endpoint L	Wireless Student Profile, AA Aruba 802.1X Wireless			
3. (Tip ANL	-	LS [Machine Authation:Ariya AD:me		l]) <i>CONTAINS</i> Staff)	AA-Aruba 802.1X	Wireless Staff Profile, [Update Endpoint Known]			
4. (Tip ANL		LS [Machine Authation:Ariya AD:me		l]) <i>CONTAINS</i> Studen)	AA-Aruba 802.1X	Wireless Student Profile, [Update Endpoint Known]			

#### Here we'll add a new rule.

#### Enforcement Policies - AA Aruba 802.1X Wireless Enforcement Policy

s	ummary Enforcement Rules	
Ru	es Evaluation Algorithm: $ullet$ Select first match $igtrianglet$ Select all matches	S
Enf	orcement Policy Rules:	
	Conditions	Actions
1.	(Authorization:Ariya AD:memberOf CONTAINS Staff)	AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint Location
2.	(Authorization:Ariya AD:memberOf CONTAINS Student)	AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireless Update Endpoint Location
3.	(Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Staff)	AA-Aruba 802.1X Wireless Staff Profile, [Update Endpoint Known]
4.	(Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Studen)	AA-Aruba 802.1X Wireless Student Profile, [Update Endpoint Known]
		Add Rule         Copy Rule         Move Up ↑         Move Down ↓         Edit Rule         Remove Rule

Rule	Rules Editor									
	Conditions									
Mate	Match ALL of the following conditions:									
	Туре	Name	Operator	Value						
1.	Tips	Role	EQUALS	all-test-group-member	e t					
2.	Click to add									
			Enforcement Profiles							
Prot	file Names:	[RADIUS] AA-Aruba 802.1X Wireless Student Profil	e Move Up † Move Down j Remove							
					Cancel					

The new rule is basically saying if Tips role is "all-test-group-member" then use the highlighted profile, and then save it.

#### Enforcement Policies - AA Aruba 802.1X Wireless Enforcement Policy

	Summary Enforcement Rules	
Rı	lles Evaluation Algorithm: $lacksquare$ Select first match $igtriangle$ Select all matches	
En	forcement Policy Rules:	
	Conditions	Actions
1.	(Tips:Role EQUALS all-test-group-member)	[RADIUS] AA-Aruba 802.1X Wireless Student Profile
2.	(Authorization:Ariya AD:memberOf CONTAINS Staff)	AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint Location
з.	(Authorization:Ariya AD:memberOf CONTAINS Student)	AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireless Update Endpoint Location
4.	(Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Staff)	AA-Aruba 802.1X Wireless Staff Profile, [Update Endpoint Known]
5.	(Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Studen)	AA-Aruba 802.1X Wireless Student Profile, [Update Endpoint Known]
	Add Rule	Copy Rule Move Up↑ Move Down↓ Edit Rule Remove Rule

K Back	to Services							Сору	Save	Cancel
Servio	es - AA Ar	uba 802.1X	Wirele	SS						
Summa	ry Service	Authentication	Roles	Enforcement						
Use Cach	ed Results:	Use cached	Roles and	l Posture attribu	es from previ	ous sessions				
Enforcem	ent Policy:	AA Aruba 802.	1X Wireless	Enforcement Polic	/	<ul> <li>Modify</li> </ul>	2	Add I	New Enfor	rcement Policy
					Enforcement	t Policy Detail	5			
Descripti	on:									
Default Profile:		AA Aruba 80	AA Aruba 802.1X Wireless Default Profile							
Rules Ev	aluation Algorit	nm: first-applicab	le							
Co	nditions						Enforcement Profiles			
1. (1	ips:Role EQUA	LS all-test-group	-member)			/	A-Aruba 802.1X Wireless Student P	rofile		
2. (/	(Authorization:Ariya AD:memberOf CONTAINS Staff)					AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint Location				
3. (/	(Authorization:Ariya AD:memberOf CONTAINS Student)						AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireles Update Endpoint Location			
4. `		LS [Machine Auth ation:Ariya AD:me				/	A-Aruba 802.1X Wireless Staff Profi	ile, [Update	Endpoint	Known]
5		LS [Machine Auth ation:Ariya AD:me			n)	/	AA-Aruba 802.1X Wireless Student P	rofile, [Upd	ate Endpo	pint Known]

#### Once this is saved, we'll reconnect using test1 user

aruba		ClearPas	ss Policy Manag	er		Menu 🗮				
Dashboard		Ionitoring » Live Monitoring » Access Tracker Access Tracker Apr 01, 2021 11:44:27 AEDT								
Access Tracker Accounting Consultation OnGuard Activity	The Access Tracker page pro	vides a real-time display		ity on the selected server or		Edit				
- Analysis & Trending - System Monitor - Profiler and Network Scan - P Audit Viewer	Filter: Request ID # Server	<ul> <li>✓ contains ✓</li> <li>Source</li> </ul>	Username	Go Clear Filter Service	Login Status	Show 20				
	1. 192.168.1.95	RADIUS	test1	AA Aruba 802.1X Wireless	ACCEPT	2021/04/01 11:43:48				

#### You'll notice that the student profile enforcement profile is being matched.

Summary Input (	Dutput Accounting								
Login Status:	ACCEPT								
Session Identifier: R0000002-01-60651744									
Date and Time: Apr 01, 2021 11:43:48 AEDT									
End-Host Identifier: A0-88-B4-50-C0-84									
Username: test1									
Access Device IP/Port:	192.168.1.57 (MD-1 / Aruba)								
Access Device Name:	7008-1								
System Posture Status:	UNKNOWN (100)								
	Policies Used -								
Service:	AA Aruba 802.1X Wireless								
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2								
Authentication Source:	AD:192.168.1.250								
Authorization Source:	Ariya AD								
Roles:	[User Authenticated], all-test-group-member								
Enforcement Profiles:	AA-Aruba 802.1X Wireless Student Profile								

#### **Request Details**

Summary	Input	Output	Accounting				
Enforcement Profiles: AA-Aruba 802.1X Wireless Student Profile							
System Posture Status: UNKNOWN (100)							
Audit Posture	Status:	UNKNOV	VN (100)				
RADIUS Res	ponse		(				
RADIUS Response							

# **3 Nested AD group Configuration – Method2**

This is the seond way of achieving the same result by using a LDAP OID for recursive retrieval of all group memberships. The OID is (1.2.840.113556.1.4.1941).

# 3.1 ClearPass Configuration

We are assuming you already have joined ClearPass to the AD domain and have configured an Authentication source for it as seen below. Now checking the attributes that were created from our first method.

aruba		ClearPass Policy Manager									
Dashboard	• Conf	figuration » Authenti	ication » Sources	» Add - Ariya AD							
Monitoring	<ul> <li>Aut</li> </ul>	Authentication Sources - Ariya AD									
A Configuration	Configuration Summary General Primary Attributes										
- Caracterization and authorization and authorization attributes											
- C Services		Filter Name		Attribute Name	Alias Name	Enabled As					
🖃 🖴 Authentication	1.			dn	UserDN	-					
- 🗘 Methods				department	Department	-					
- 🎝 Sources				title	Title	-					
Single Sign-On (SSO)	(SSO) Authent			company	company	-					
Local Users				memberOf	memberOf	-	Đ	÷			
- Di Endpoints				telephoneNumber	Phone	-					
- 🛱 Static Host Lists				mail	Email	-					
- 🛱 Roles				displayName	Name	-					
- 🎝 Role Mappings				accountExpires	Account Expires	-					
⊕ ♥ Posture	2.			cn	SubGroups	-		-			
Enforcement		SubGroup		memberOf	SubGroupmemberOf	-	Ð	Ť			
- 🛱 Policies 🛱 Profiles	3.			dNSHostName	HostName	-					
Network		Machine		operatingSystem	OperatingSystem	-	1	-			
- Devices				operatingSystemServicePack	OSServicePack	-					
Device Groups	4.	Onboard Device O	wner	memberOf	Onboard memberOf	-	1	÷			
- 🎝 Proxy Targets	5.	Onboard Device O	wner Group	cn	Onboard Groups	-	1	ŵ			
- 🎝 Event Sources	6.			cn	OneLevelUp	-		-			
- n Network Scan		OneLevelUp		1 07	a i lii l af			÷			

#### This method requires to add just one attribute. The Filter query that we'll use is

#### Filter Query = (member:1.2.840.113556.1.4.1941:=%{UserDN})

aruba		Clear	Pass Policy Ma	nager			Menu
Dashboard	• Configuration » A	Authentication » Sources » Add -	Ariya AD				
Monitoring	Configure Filter				0		
Configuration	Configuration At	tributes Browse Filter					
- 🛱 Service Templates & Wizards							
- 🛱 Services	Filter Name:	AllGroups					
	Filter Query:	(member:1.2.840.113556	5.1.4.1941:=%{UserDN})				
- 🛱 Methods							Br #
- 🗘 Sources							197 =
E- 2 Identity	Name	Alias Name	Data type	Enabled As			
– 🛱 Single Sign-On (SSO)	1. cn	Nested Groups	String	Role	8		
- 🎝 Local Users	2. Click to add						
- 🛱 Endpoints	2. Onor to bud						
- 🎝 Static Host Lists							
- 🛱 Roles							<u>18</u> a
- 🎝 Role Mappings							
🖅 🖶 Posture							6/ 1
選 Enforcement							
- 🛱 Policies							Gr #
- 🛱 Profiles							
							Er 🗉
- 🗘 Devices							
- 🛱 Device Groups							<u></u>
- Proxy Targets					Save Close	2	ir
Event Sources							Add More Filters
- 🛱 Network Scan							Fidd more Filters
- Policy Simulation	Y Sack to Aut	hentication Sources			Clear	Cache Copy	Save Cancel

Configuration » Authentication » Sources » Add - Ariya AD

#### Authentication Sources - Ariya AD

	mmary General Primary	Attributes				
		department	Department	-		
		title	Title	-		
		company	company	-		
	Authentication	memberOf	memberOf	-	1	, û
		telephoneNumber	Phone	-		
		mail	Email	-		
		displayName	Name	-		
		accountExpires	Account Expires	-		
2.	Cult Craun	cn	SubGroups	-	D	, <del>1</del>
	SubGroup	memberOf	SubGroupmemberOf	-	19	· Ш
3.		dNSHostName	HostName	-		
	Machine	operatingSystem	OperatingSystem	-	Ð	Û
		operatingSystemServicePack	OSServicePack	-		
4.	Onboard Device Owner	memberOf	Onboard memberOf	-	i)	Û
5.	Onboard Device Owner Group	cn	Onboard Groups	-	1	Û
6.	Onderselle	cn	OneLevelUp	-		, î
	OneLevelUp	memberOf	OneLevelUpmemberOf	-	12	· Ш
7.	AllGroups	cn	Nested Groups	Role	÷	, Û
	_				Add More	Filter
р	Back to Authentication Source			Clear Cache Copy	Save	Canc

This will enable ClearPass to present "Nested Group" as an option for AD authorization. Remember that our user is "test1" which is memberof

→ "test-users" group that is in the

• memberof "all-test-users" group.

Now for this method we don't need to do any role mapping you can directly check for it in the enforcement policy.

### 3.2 Testing

We'll use the same win10 laptop connecting to the dot1x SSID. The username we are using is "test1" which is successfully authenticated. Note the Role that is matched in addition to "all-test-group-member".

CCESS Tracker Apr 1 Request Details	8, 2021 14:58:52 AEST								
Summary Input	Output Accounting								
Login Status:	ACCEPT	1							
Session Identifier:	000001-01-607bbb7d								
Date and Time:	Apr 18, 2021 14:54:24 AEST								
End-Host Identifier:	A0-88-B4-50-C0-84								
Username:	test1								
Access Device IP/Port:	192.168.1.10 (InstantVC-Lab / Aruba)								
Access Device Name:	InstantVC								
System Posture Status:	UNKNOWN (100)								
	Policies Used -								
Service:	AA Aruba 802.1X Wireless								
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2								
Authentication Source:	AD:192.168.1.250								
Authorization Source:	Ariya AD	1							
Roles:	[User Authenticated], all-test-group-member, all-test-users, test-users								
Enforcement Profiles:	AA-Aruba 802.1X Wireless Student Profile								
<ul> <li>Showing 1 of 1-2 re</li> </ul>	cords ► ► Change Status Show Configuration Export Show Logs Clos	е							

Again, "all-test-users" and "test-users" are the nested AD groups. In the authorisation section we'll see the "Nest Group" attributes.

Summary	Input	Output	Accounting	RADIUS CoA		
Username:		test1				
End-Host Ide	entifier:	A0-88-B4-	50-C0-84			
Access Devic	e IP/Port:	192.168.1	.10	(InstantVC-Lab / Aruba)		
RADIUS Re	quest				۲	
Authorizatio	n Attribute	s			۲	
Authorizati	on:Ariya A	D:Account	Expires	9223372036854775807 [30828-09-14 12:48:05 AEST]		
Authorizati	on:Ariya A	D:member	Of	CN=test-users,CN=Users,DC=wlan,DC=net		
Authorizati	on:Ariya A	D:Name		test		
Authorizati	on:Ariya A	D:Nested (	Groups	all-test-users, test-users		
Authorizati	on:Ariya A	D:OneLeve	lUp	all-test-users		
Authorizati	on:Ariya A	D:SubGrou	pmemberOf	CN=all-test-users,CN=Users,DC=wlan,DC=net		
Authorization:Ariya AD:SubGroups test-users						
Authorizati	on:Ariya A	D:UserDN		CN=test1,CN=Users,DC=wlan,DC=net		

We also see the previous method's attribute values with red underline as shown above and finally the output tab that shows ClearPass sending back Aruba-user-role of Student.

Summary	Input	Output	Accounting	
Enforcement	Profiles:	AA-Arub	a 802.1X Wireless Student Profile	
System Postu	re Status:	UNKNOV	/N (100)	
Audit Posture	Status:	UNKNOV	/N (100)	
RADIUS Res	ponse		$\odot$	
Radius:Arul	ba:Aruba-l	User-Role	Student	

The main point here is, instead of having a role-mapping policy as with the previous method, you can directly modify the enforcement policy to check of the AD-Authorisation attribute called "Nested Groups"

Here the modified dot1x service.

-

Ser	Services - AA Aruba 802.1X Wireless									
Su	mmary Service	Authentication	Roles	Enforcement						
Nam	e:	AA Aruba 802.1)	Wireless							
Description: To authenticate users to an Aruba wireless network via 802.1X.										
Туре	Type: Aruba 802.1X Wireless									
Status: Enabled										
Moni	tor Mode:	🗆 Enable to m	onitor ne	twork access with	out	enforcement				
More	e Options:	🗆 Authorizatio	n 🗌 Pos	ture Compliance		Audit End-hosts 🛛 Profile Endpoints	Accour	nting Proxy		
						Service Rule				
Matc	hes 🔿 ANY or 🖲 A	LL of the followin	g conditio	ons:						
	Туре		Nam	e		Operator		Value		
1.	Radius:IETF	F NAS-Port-Type EQUALS Wireless-802.11 (19) 🖷							ĒÐ	Ť
2.	Radius:IETF	Service-Type BELONGS_TO Login-User (1), Framed-User (2), Authenticate-Only (8)								
3.	Radius:Aruba		Aruba-Essid-Name EQUALS school 🗎 🖆							
4.	Click to add									

Summary	Service	Authentication	Roles	Enforcement		
Authentication	n Methods:	[EAP PEAP]		1	^	Add New Authentication Method
		[EAP TLS]				Move Up ↑
						Move Down ↓
						Remove
						View Details
						Modify
					~	
		Select to Add			~	
Authentication	n Sources:	Ariya AD [Activ	e Directory	) (	$\sim$	Add New Authentication Source
						Move Up ↑
						Move Down ↓
						Remove
						View Details
						Modify
					~	
		Select to Add			~	▼
Strip Usernan	ne Rules:	🗆 Enable to sp	ecify a co	omma-separated	d list	ist of rules to strip username prefixes or suffixes
Service Certif	icate:	Select to Add	-		~	View Certificate Details

#### Note that here we have removed the role-mapping policy.

Summary	Service	Authentication	Roles	Enforcement		
Role Mapping	Policy:	Select			~ Modify	Add New Role Mapping Policy
					Role Mapping Policy Details	
Description:		-				
Default Role:		-				
Rules Evaluati	ion Algorith	m: -				
Conditi	ons				Role	

And here we have modified the first rule to check the new attribute "Nested Groups" which we added to the authentication source.

Summa	ry Service	Authentication	Roles	Enforcement			
Use Cached Results: Use cached Roles and Posture attributes from previo					from previous sessions		
Enforcem	ent Policy:	AA Aruba 802.	1X Wireless	Enforcement Policy	Modify     Add New Enforce	ement Policy	
	Enforcement Policy Details						
Descripti	on:						
Default P	rofile:	AA Aruba 802	2.1X Wire	less Default Profil			
Rules Evaluation Algorithm: first-applicable							
Co	nditions				Enforcement Profiles		
1. <mark>(/</mark>	uthorization:Ar	riya AD:Nested Gro	oups EQU	IALS test-users)	AA-Aruba 802.1X Wireless Student Profile		
2. (/	uthorization:Ar	riya AD:memberOf	CONTAI	NS Staff)	AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X W Update Endpoint Location	ireless	
3. (/	uthorization:Ar	riya AD:memberOf	CONTAI	NS Student)	AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Update Endpoint Location	Wireless	
4. `	•	LS [Machine Auth ation:Ariya AD:me			AA-Aruba 802.1X Wireless Staff Profile, [Update Endpoint Ki	nown]	
5. (1	•	LS [Machine Auth		]) CONTAINS Stude	AA-Aruba 802.1X Wireless Student Profile, [Update Endpoin	t Known]	

#### Now we'll test again with the same username.

# Access Tracker Apr 18, 2021 15:16:20 AEST The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain. The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain. Edit The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain. Edit

Filter:	Request ID	∼ contains ~	🛨 Go Cl	ear Filter		Show 20 v records
#	Server	Source	Username	Service	Login Status	Request Timestamp 🔻
1.	<mark>192.168.1.95</mark>	RADIUS	test1	AA Aruba 802.1X Wireless	ACCEPT	2021/04/18 15:16:03
2.	192.168.1.95	RADIUS	test1	AA Aruba 802.1X Wireless	ACCEPT	2021/04/18 14:54:24

#### Checking the access tracker request

Summary Input (	Dutput Accounting				
Login Status:	ACCEPT				
Session Identifier:	R0000002-01-607bc092				
Date and Time:	Apr 18, 2021 15:16:03 AEST				
End-Host Identifier:	A0-88-B4-50-C0-84				
Username:	test1				
Access Device IP/Port:	192.168.1.10 (InstantVC-Lab / Aruba)				
Access Device Name:	InstantVC				
System Posture Status:	UNKNOWN (100)				
	Policies Used -				
Service:	AA Aruba 802.1X Wireless				
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2				
Authentication Source:	AD:192.168.1.250				
Authorization Source:	Ariya AD				
Roles:	[User Authenticated], all-test-users, test-users				
Enforcement Profiles:	AA-Aruba 802.1X Wireless Student Profile				

You'll notice that "all-test-group-member" is not listed under Roles because we did not have the role mapping policy. And below is the authorisation section of the request as computed by ClearPass

SummaryInputOutputAccountingUsername:test1End-Host Identifie:A0-88-B4-50-C0-84Access Device IP/Port:192.168.1.10(InstantVC-Lab / Aruba)RADIUS RequestAuthorization AttributesAuthorization: Ariya AD: Account Expires9223372036854775807 [30828-09-14 12:48:05 AEST]Authorization: Ariya AD: Account Expires9223372036854775807 [30828-09-14 12:48:05 AEST]Authorization: Ariya AD: NemeberOfCN=test-users, CN=Users, DC=wlan, DC=netAuthorization: Ariya AD: NametestAuthorization: Ariya AD: Nested Groupsall-test-users, test-usersAuthorization: Ariya AD: UserDNCN=test-users, DC=wlan, DC=netComputed AttributesC	Request Details					
End-Host Identifier:       A0-88-B4-50-C0-84         Access Device IP/Port:       192.168.1.10       (InstantVC-Lab / Aruba)         RADIUS Request         Authorization Attributes         Authorization:Ariya AD:Account Expires       9223372036854775807 [30828-09-14 12:48:05 AEST]         Authorization:Ariya AD:Account Expires       9223372036854775807 [30828-09-14 12:48:05 AEST]         Authorization:Ariya AD:MemberOf       CN=test-users,CN=Users,DC=wlan,DC=net         Authorization:Ariya AD:Nested Groups       all-test-users test-users         Authorization:Ariya AD:Nested Groups       all-test-users,DC=wlan,DC=net         Authorization:Ariya AD:Nested Groups       all-test-users,DC=wlan,DC=net	Summary Input	Output	Account	ing		
Access Device IP/Port:       192.168.1.10       (InstantVC-Lab / Aruba)         RADIUS Request         Authorization Attributes       •         Authorization: Ariya AD: Account Expires       9223372036854775807 [30828-09-14 12:48:05 AEST]       •         Authorization: Ariya AD: Account Expires       9223372036854775807 [30828-09-14 12:48:05 AEST]       •         Authorization: Ariya AD: MemberOf       CN=test-users, CN=Users, DC=wlan, DC=net       •         Authorization: Ariya AD: Name       test       •         Authorization: Ariya AD: Nested Groups       all-test-users, test-users       •         Authorization: Ariya AD: Nested Groups       cN=test1, CN=Users, DC=wlan, DC=net       •	Username:	test1				
RADIUS Request       Image: Constraint of the second	End-Host Identifier:	A0-88-B4-	-50-C0-84	1		
Authorization Attributes       •         Authorization: Ariya AD: Account Expires       9223372036854775807 [30828-09-14 12:48:05 AEST]         Authorization: Ariya AD: memberOf       CN=test-users, CN=Users, DC=wlan, DC=net         Authorization: Ariya AD: Name       test         Authorization: Ariya AD:Nested Groups       all-test-users, test-users         Authorization: Ariya AD:UserDN       CN=test1, CN=Users, DC=wlan, DC=net	Access Device IP/Port:	192.168.1	10	(InstantVC-Lab / Aruba)		
Authorization Attributes       9223372036854775807 [30828-09-14 12:48:05 AEST]         Authorization:Ariya AD:MemberOf       CN=test-users,CN=Users,DC=wlan,DC=net         Authorization:Ariya AD:Name       test         Authorization:Ariya AD:Nested Groups       all-test-users, test-users         Authorization:Ariya AD:UserDN       CN=test1,CN=Users,DC=wlan,DC=net	RADIUS Request	RADIUS Request				
Authorization:Ariya AD:memberOf       CN=test-users,CN=Users,DC=wlan,DC=net         Authorization:Ariya AD:Name       test         Authorization:Ariya AD:Nested Groups       all-test-users, test-users         Authorization:Ariya AD:UserDN       CN=test1,CN=Users,DC=wlan,DC=net	Authorization Attribute	es			۲	
Authorization:Ariya AD:Name       test         Authorization:Ariya AD:Nested Groups       all-test-users, test-users         Authorization:Ariya AD:UserDN       CN=test1,CN=Users,DC=wlan,DC=net	Authorization: Ariya	AD:Account	Expires	9223372036854775807 [30828-09-14 12:48:05 AEST]		
Authorization:Ariya AD:Nested Groups       all-test-users, test-users         Authorization:Ariya AD:UserDN       CN=test1,CN=Users,DC=wlan,DC=net	Authorization: Ariya AD: memberOf			CN=test-users,CN=Users,DC=wlan,DC=net		
Authorization:Ariya AD:UserDN         CN=test1,CN=Users,DC=wlan,DC=net	Authorization: Ariya	AD:Name	1	test		
	Authorization: Ariya	AD:Nested (	Groups a	all-test-users, test-users		
Computed Attributes	Authorization: Ariya /	AD:UserDN		CN=test1,CN=Users,DC=wlan,DC=net		
	Computed Attributes				۲	

I < Showing 1 of 1-3 records ►► Change Status Show Configuration Export Show Logs Close

And the output tab that shows the same user role is sent as with the previous method.

Summary	Input	Output	Accounting			
Enforcement	Profiles:	AA-Arub	802.1X Wireless Student Profile			
System Postu	re Status		(100)			
Audit Posture	Status:	UNKNOWN (100)				
RADIUS Response						
Radius:Aruba:Aruba-User-Role Student						