Contents

1.1 Revision History

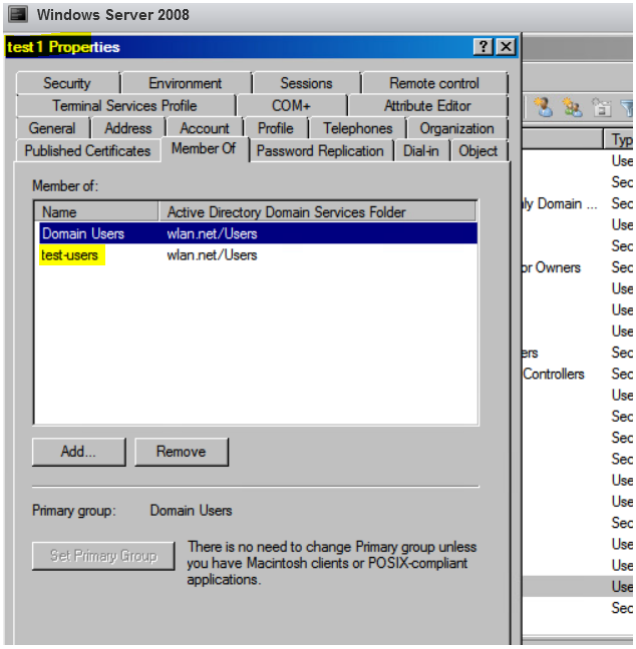
DATE	VERSION	EDITOR	CHANGES
02 Apr 2021	0.1	Ariya Parsamanesh	Initial creation
18 Apr 2021	0.2	Ariya Parsamanesh	Added the second method

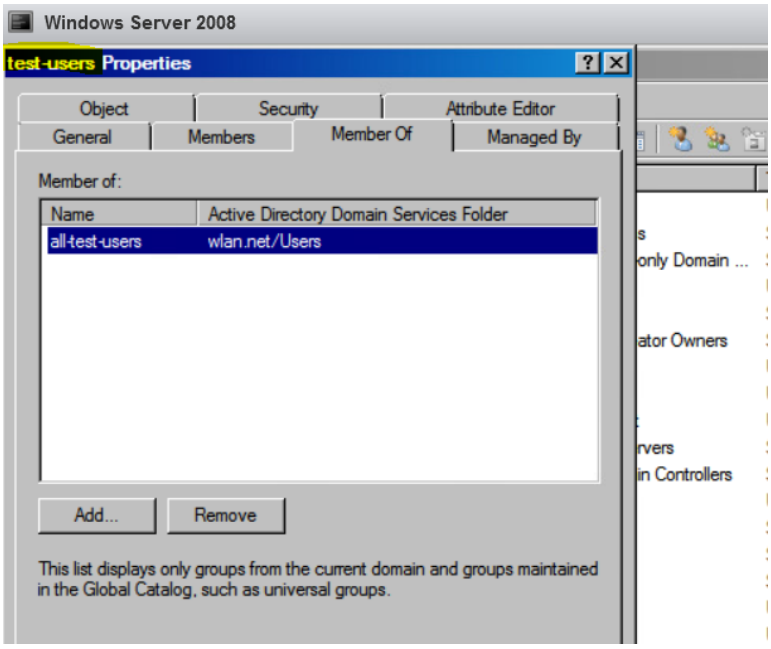
2 Nested AD group Configuration – Method1

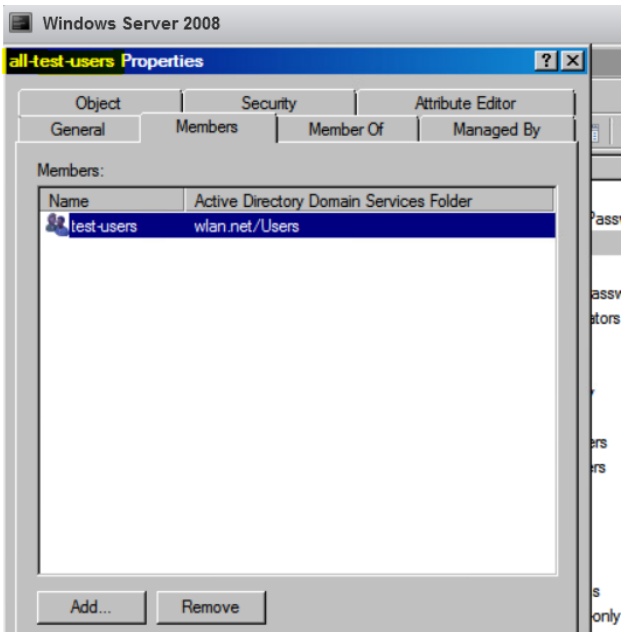
Here we are going create a ClearPass enforcement policy to check if the user is member of nested or higher level AD group. There are many cases that the users are member of a sub group that are all part of a higherlevel group and you want to create a enforcement policy with fewer rules to check for the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



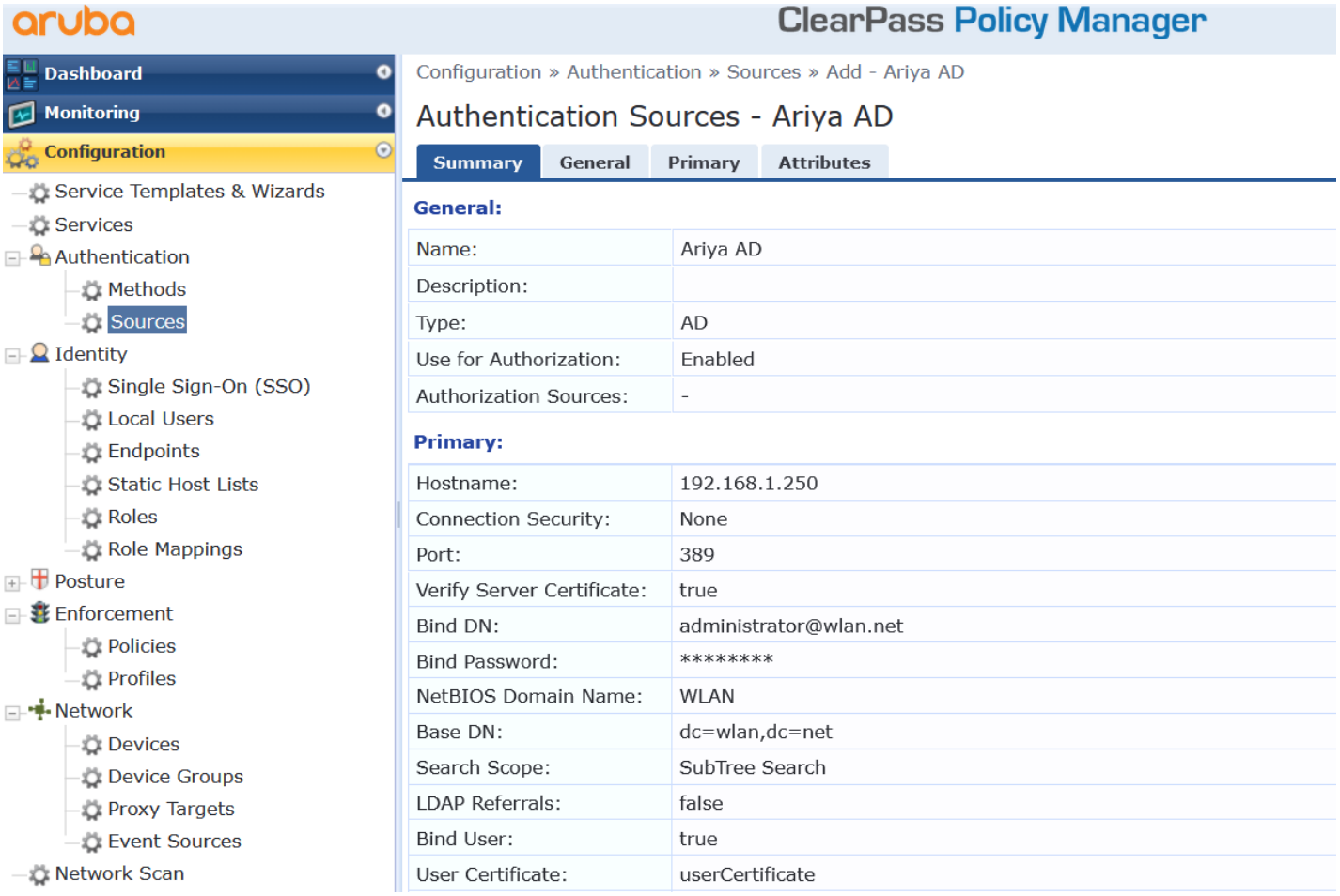




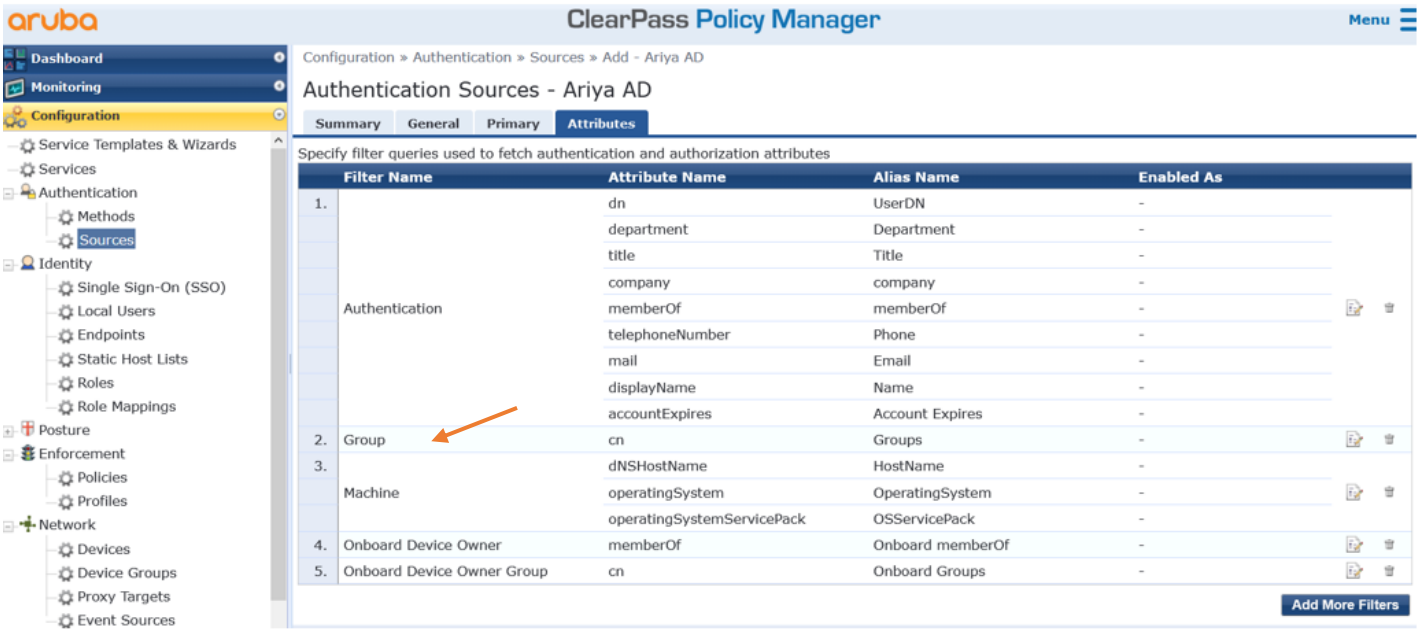
ClearPass can check if the test1 is memberof “test-users” but the condition will fail for checking memberof “all-test-users” group. So, the aim here is to be able to check if the user is in a sub-group under “all-test-users” group.

2.2 ClearPass Configuration

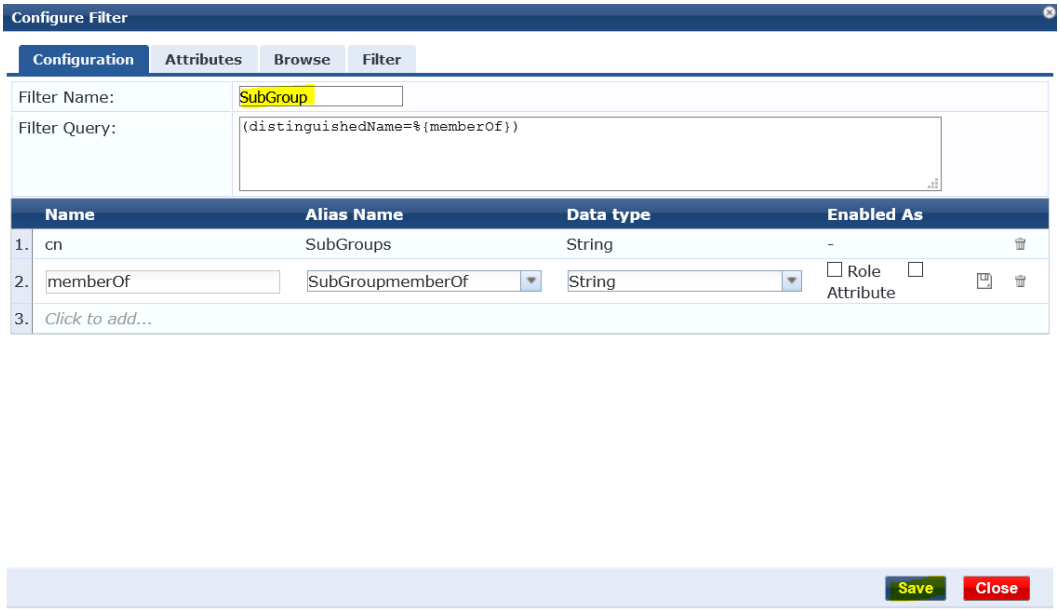
We are assuming you already have joined ClearPass to the AD domain and have configured an Authentication source for it as seen below.



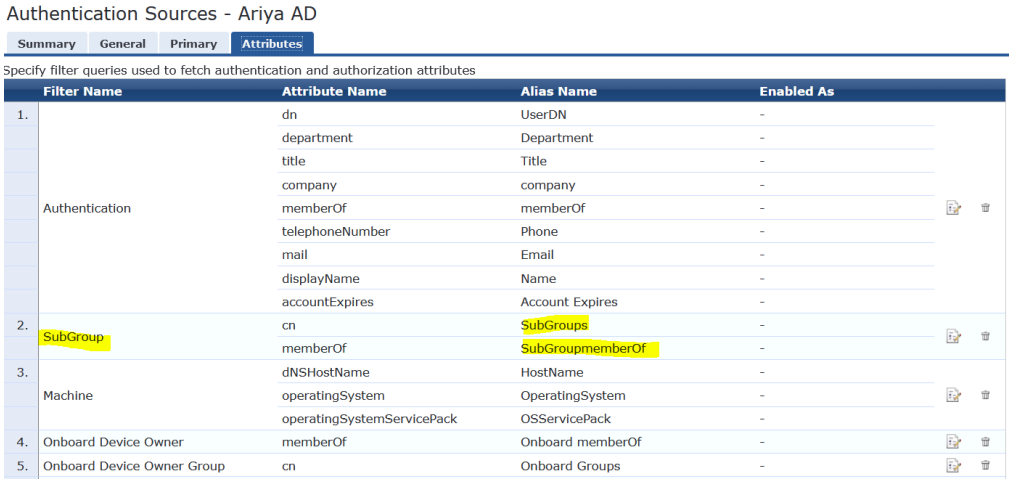
Now checking the attributes that were created by default when you configured the authentication source.



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”.

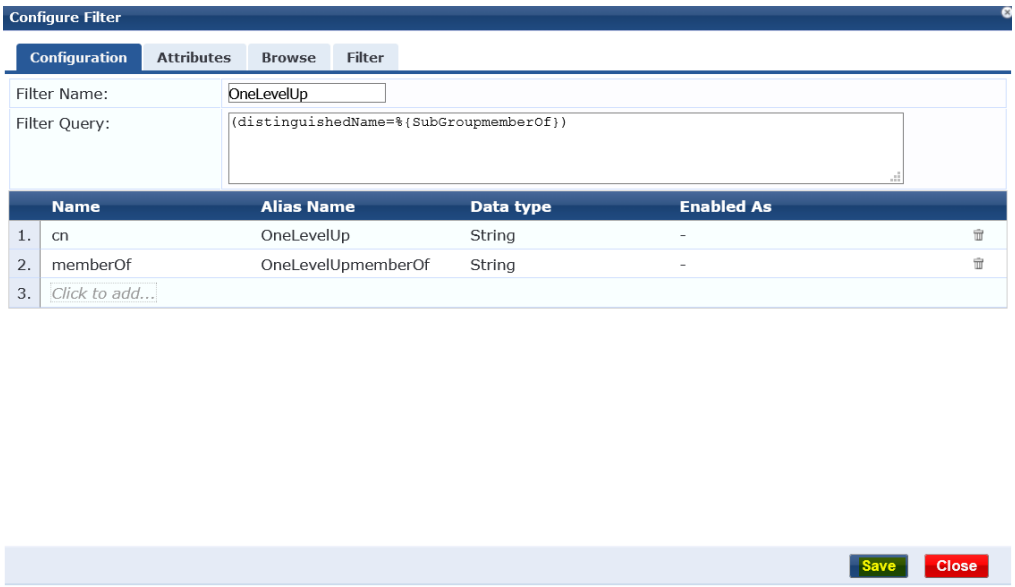


Then add/modify attributes to look like what is shown above. The name must be "memberOf" (it is case sensitive) and the Alias Name should be "SubGroupmemberOf". So, when you save it, this is what you should get.



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.



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

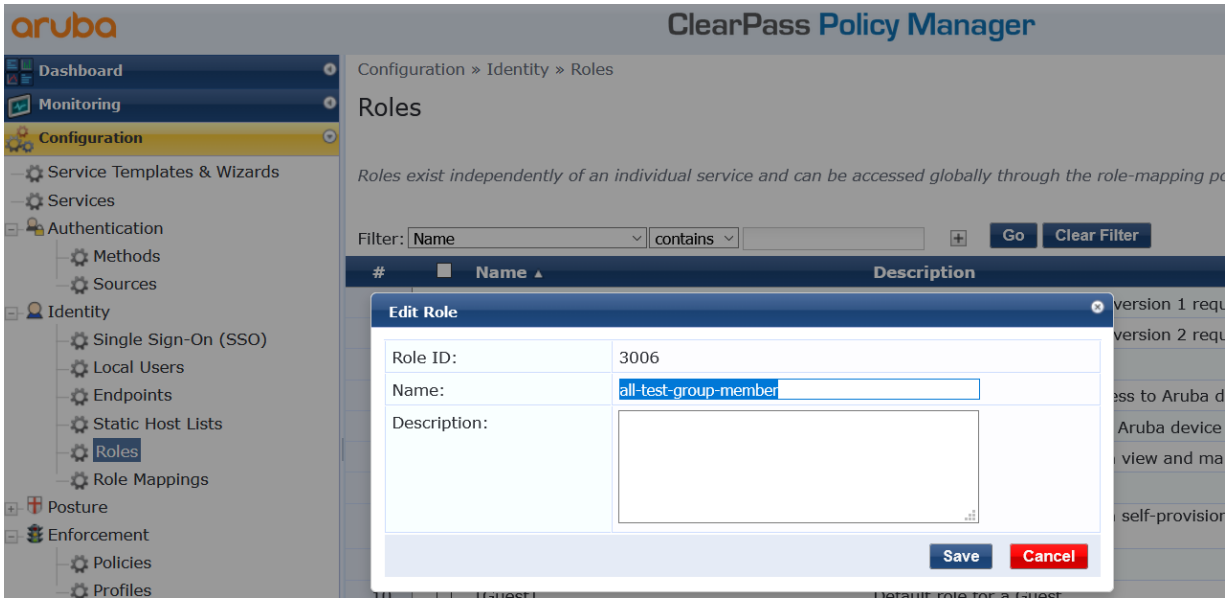
Summary | General | Primary | Attributes

Specify filter queries used to fetch authentication and authorization attributes

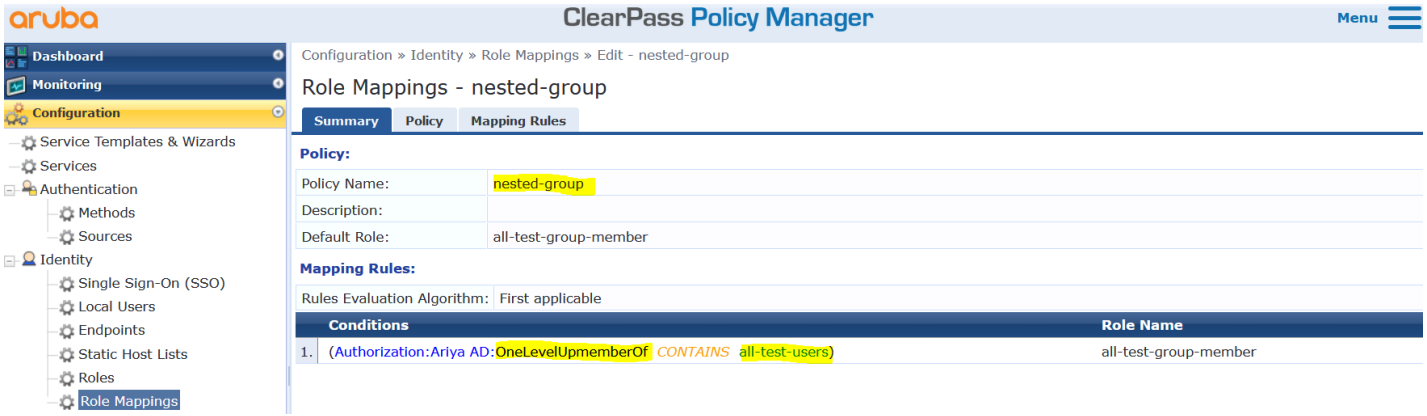
	Filter Name	Attribute Name	Alias Name	Enabled As
1.	Authentication	dn	UserDN	-
		department	Department	-
		title	Title	-
		company	company	-
		memberOf	memberOf	-
		telephoneNumber	Phone	-
		mail	Email	-
		displayName	Name	-
		accountExpires	Account Expires	-
2.	SubGroup	cn	SubGroups	-
		memberOf	SubGroupmemberOf	-
3.	Machine	dNSHostName	HostName	-
		operatingSystem	OperatingSystem	-
		operatingSystemServicePack	OSServicePack	-
4.	Onboard Device Owner	memberOf	Onboard memberOf	-
5.	Onboard Device Owner Group	cn	Onboard Groups	-
6.	OneLevelUp	cn	OneLevelUp	-
		memberOf	OneLevelUpmemberOf	-

Back to Authentication Sources | Clear Cache | Copy | Save | Cancel

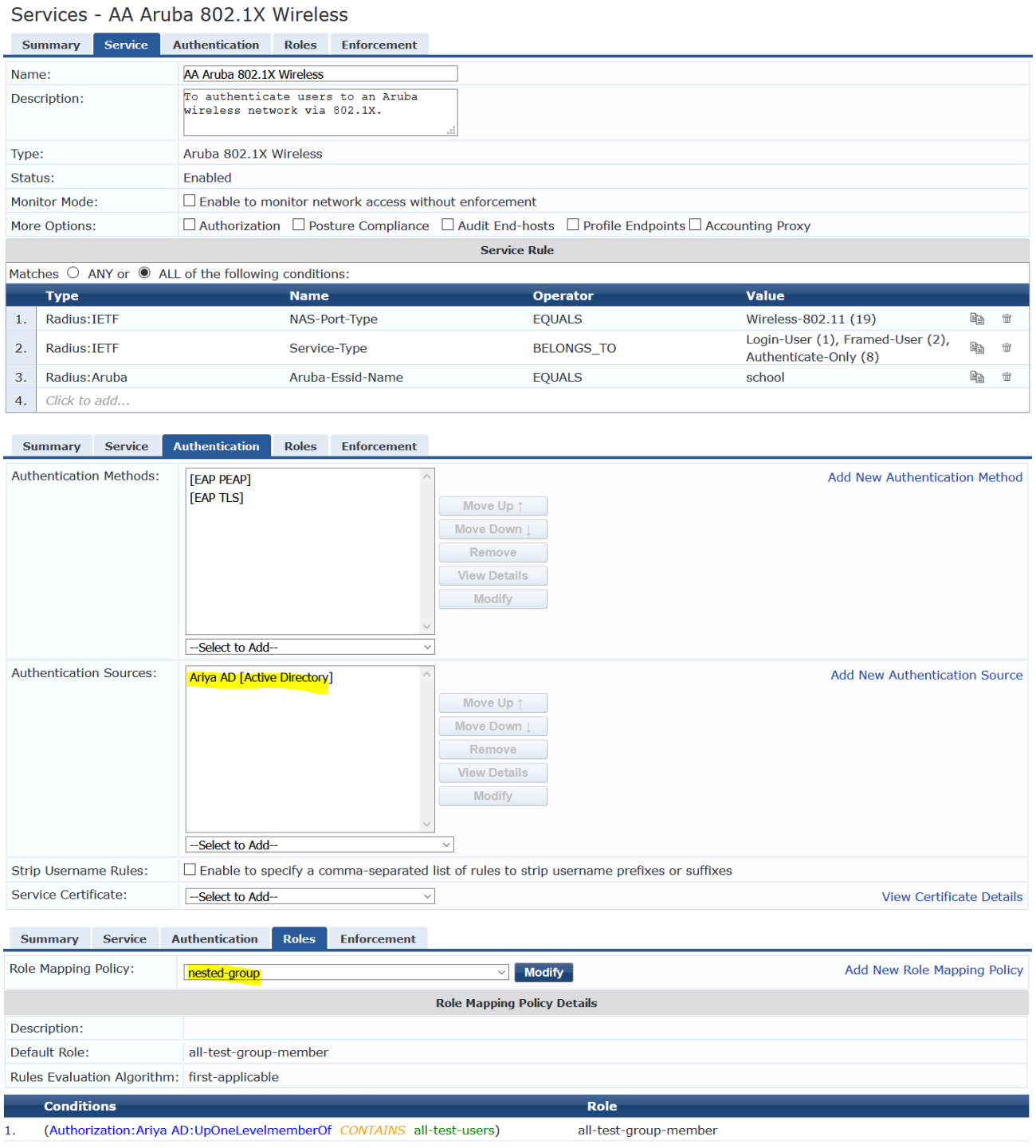
Now for ClearPass policies to use these new attributes, we need Role Mapping to map the attributes to a TIPS role that then gets referenced in the enforcement policy. First create a Role called “all-test-group-member”



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



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



Summary | Service | Authentication | Roles | Enforcement

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	AA Aruba 802.1X Wireless Enforcement Policy [Modify] Add New Enforcement Policy

Enforcement Policy Details

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

	Conditions	Enforcement Profiles
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]

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”

Access Tracker Apr 01, 2021 12:06:26 AEDT

Request Details

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000004-01-60651c8d
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

Showing 1 of 1-10 records | Change Status | Show Configuration | Export | Show Logs | Close

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

Access Tracker Apr 01, 2021 12:06:26 AEDT

Request Details

Summary | Input | Output | Accounting

Username:	test1
End-Host Identifier:	A0-88-B4-50-C0-84
Access Device IP/Port:	192.168.1.57 (MD-1 / Aruba)

RADIUS Request

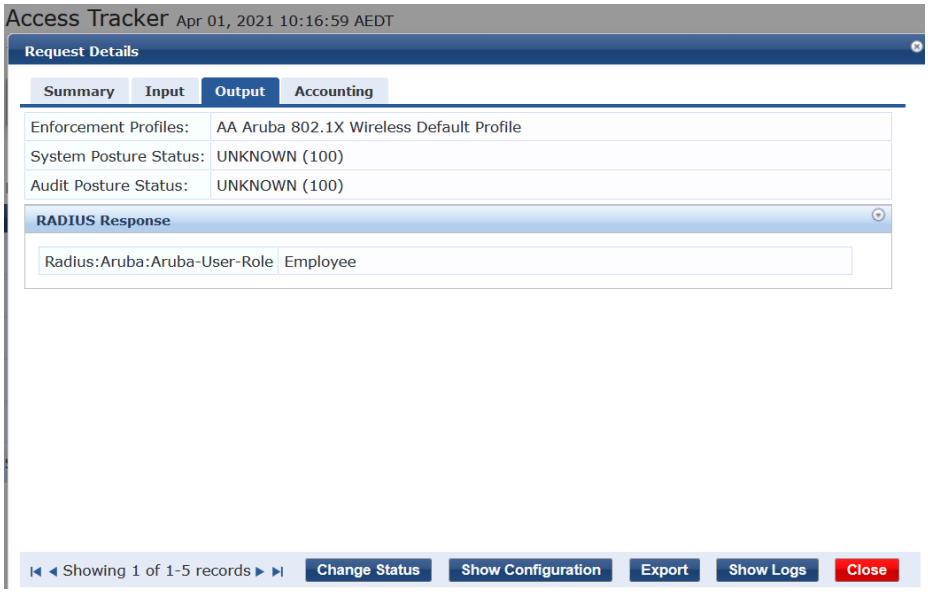
Authorization Attributes

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:OneLevelUp	all-test-users
Authorization:Ariya AD:SubGroupmemberOf	CN=all-test-users,CN=Users,DC=wlan,DC=net
Authorization:Ariya AD:SubGroups	test-users
Authorization:Ariya AD:UserDN	CN=test1,CN=Users,DC=wlan,DC=net

Computed Attributes

Showing 1 of 1-10 records | Change Status | Show Configuration | Export | Show Logs | Close

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.



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 Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	AA Aruba 802.1X Wireless Enforcement Policy [Modify] Add New Enforcement Policy

Enforcement Policy Details

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

	Conditions	Enforcement Profiles
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]

Here we’ll add a new rule.

Enforcement Policies - AA Aruba 802.1X Wireless Enforcement Policy

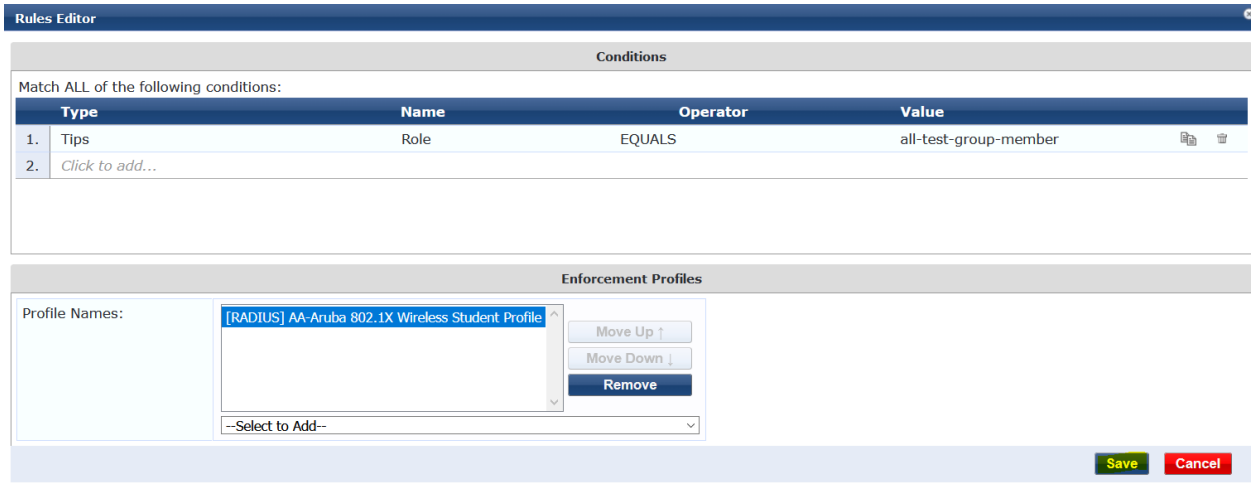
Summary | Enforcement | Rules

Rules Evaluation Algorithm: ◉ Select first match ○ Select all matches

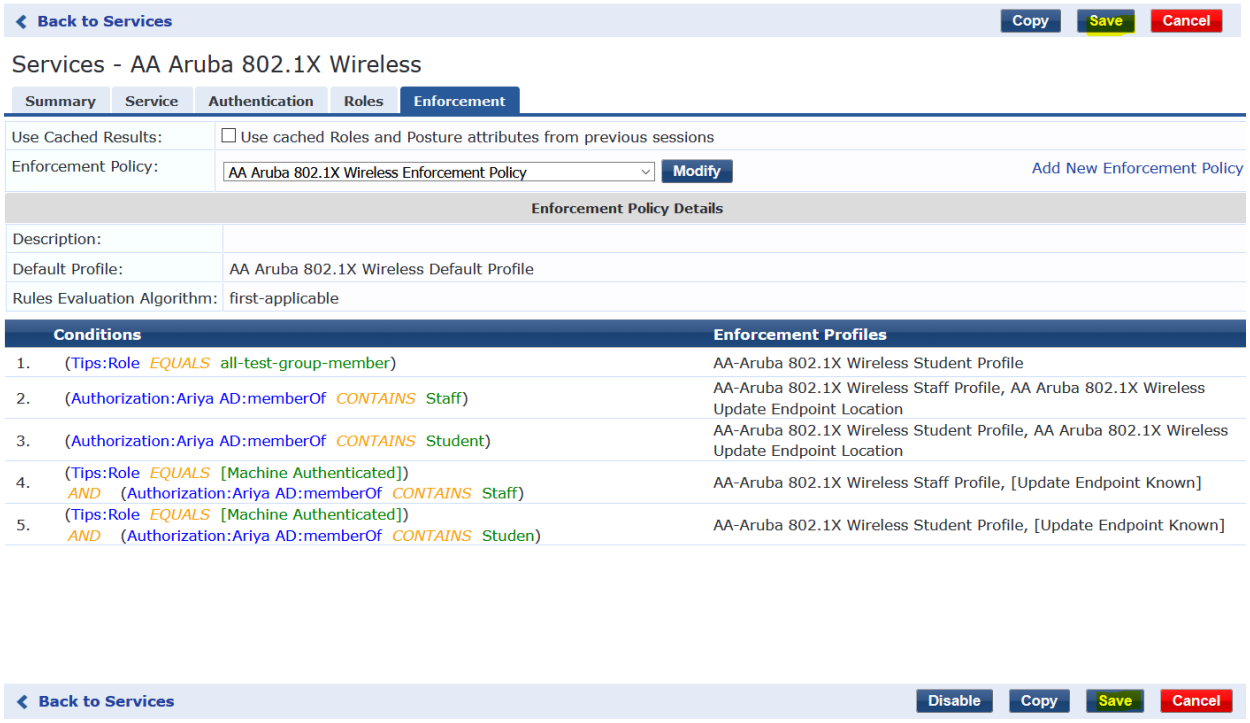
Enforcement Policy Rules:

	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]

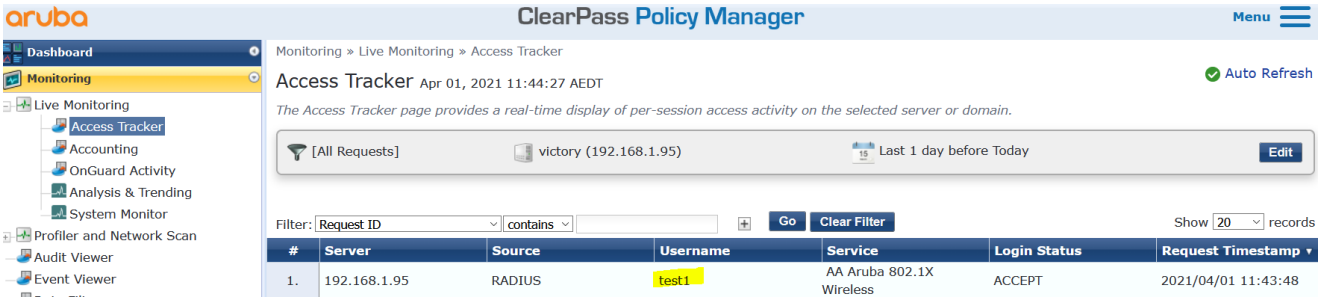
Add Rule | Copy Rule | Move Up ↑ | Move Down ↓ | Edit Rule | Remove Rule



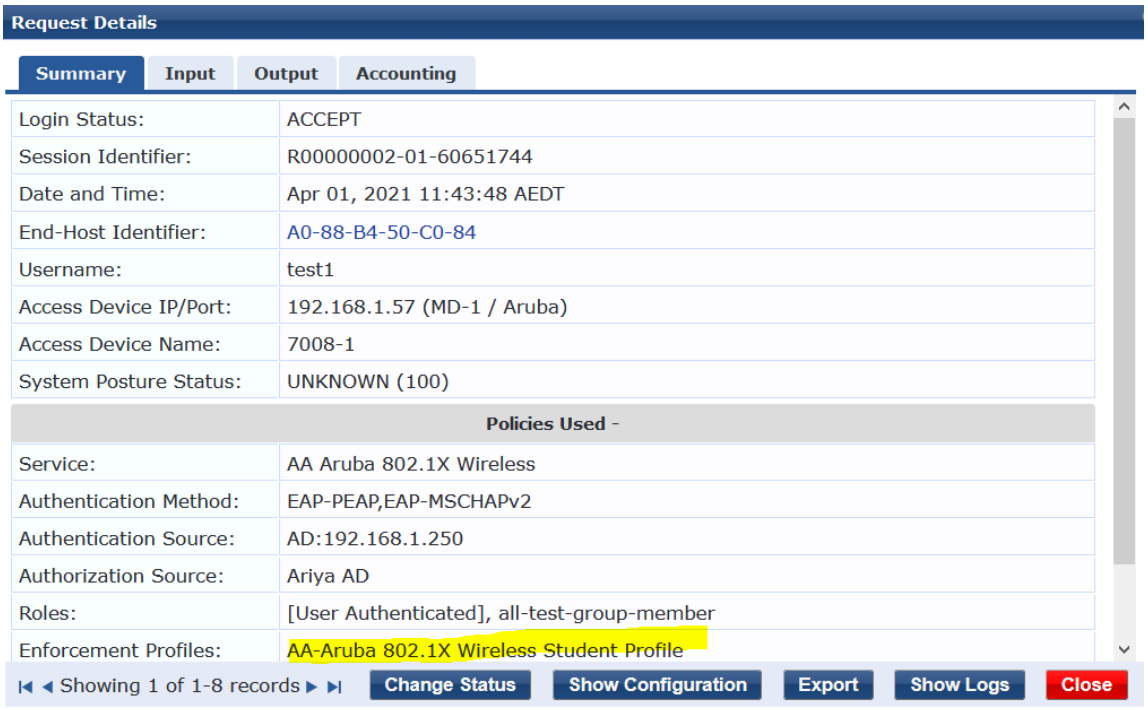
The new rule is basically saying if Tips role is “all-test-group-member” then use the highlighted profile, and then save it.

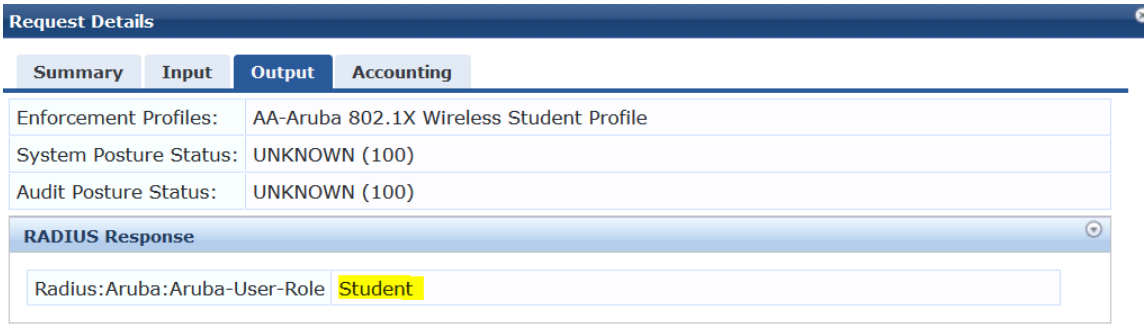


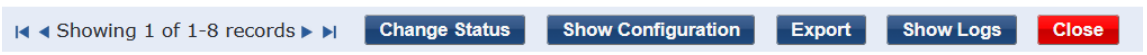
Once this is saved, we'll reconnect using test1 user



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





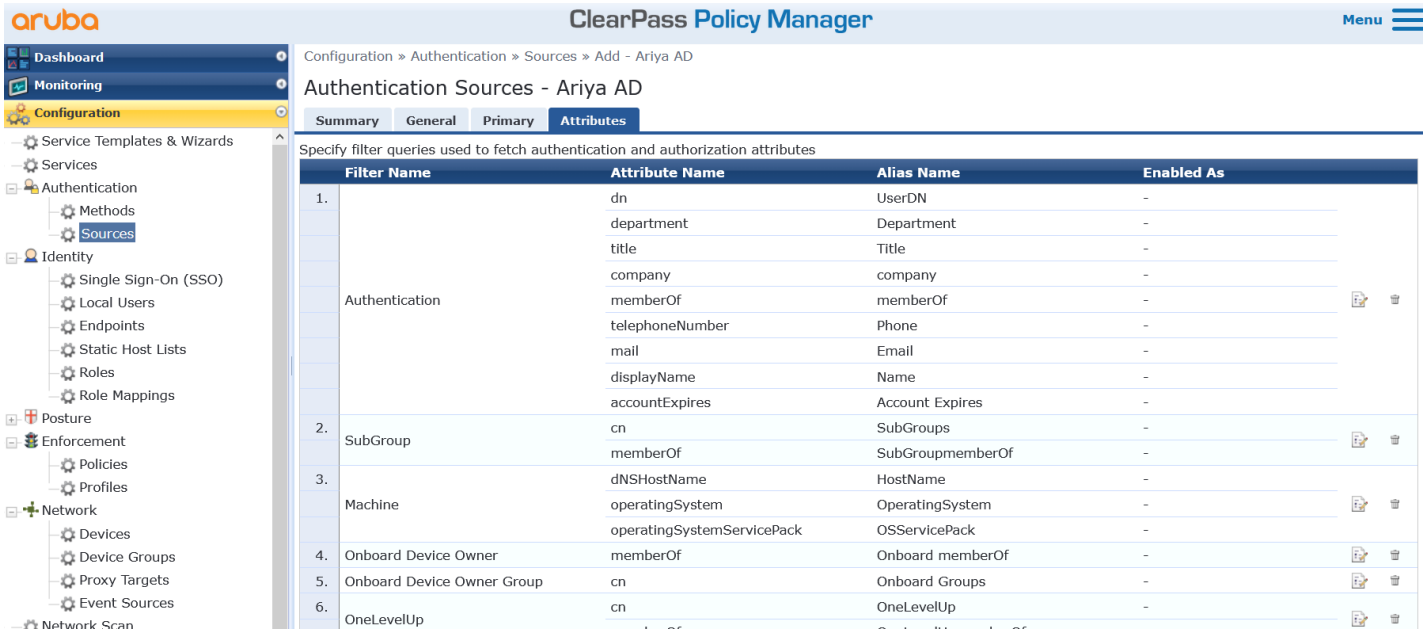


3 Nested AD group Configuration – Method2

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).

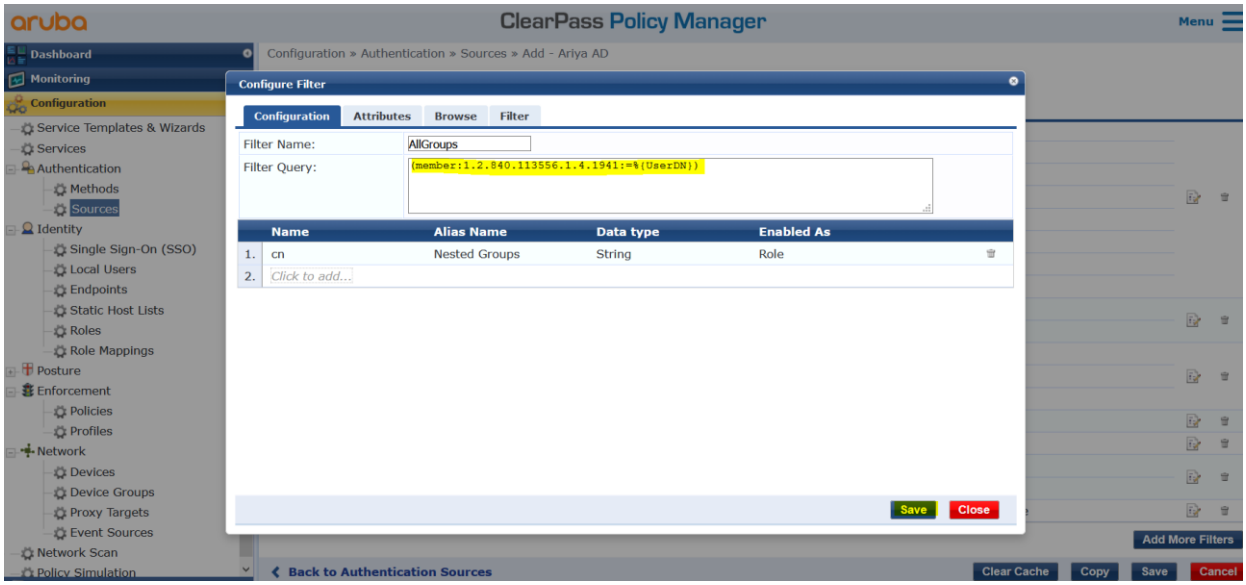
3.1 ClearPass Configuration

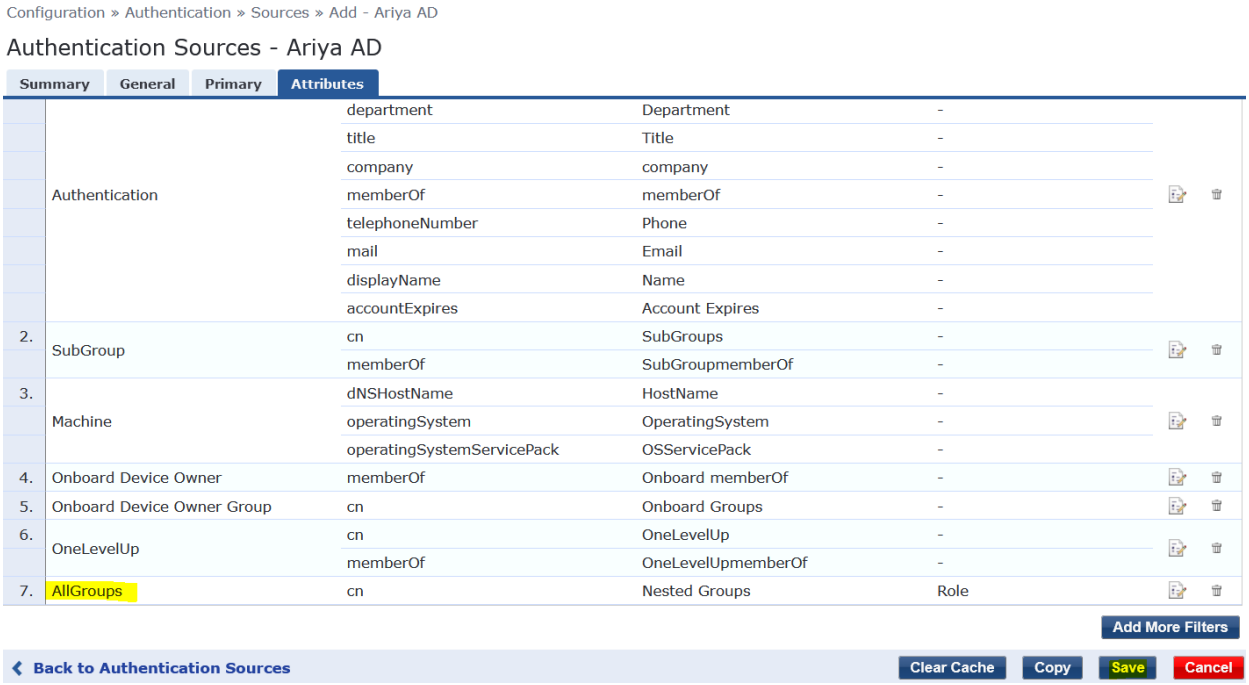
We are assuming you already have joined ClearPass to the AD domain and have configured an Authentication source for it as seen below. Now checking the attributes that were created from our first method.



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})
```





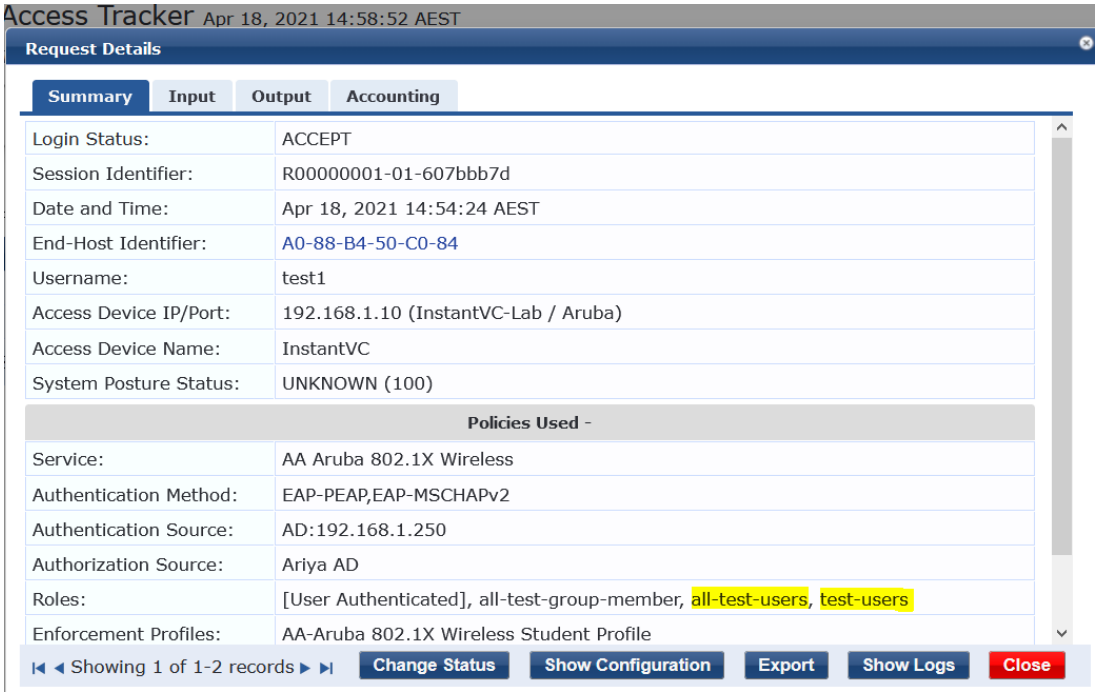
This will enable ClearPass to present “Nested Group” as an option for AD authorization. Remember that our user is “test1” which is memberof

- ➔ “test-users” group that is in the
  - memberof “all-test-users” group.

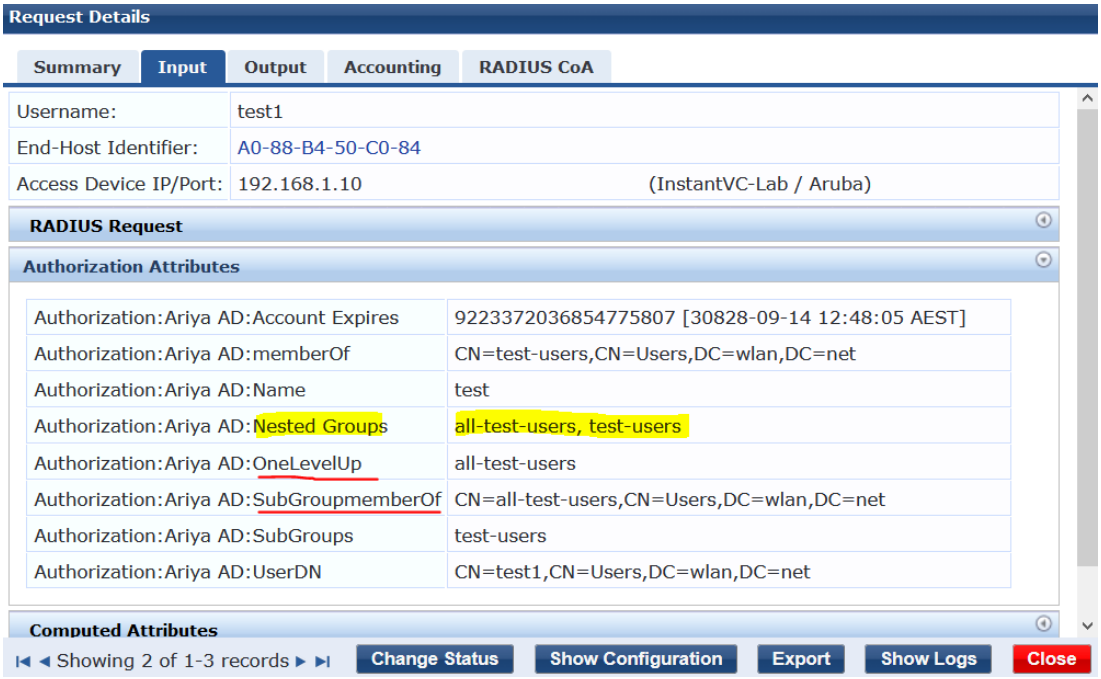
Now for this method we don’t need to do any role mapping you can directly check for it in the enforcement policy.

3.2 Testing

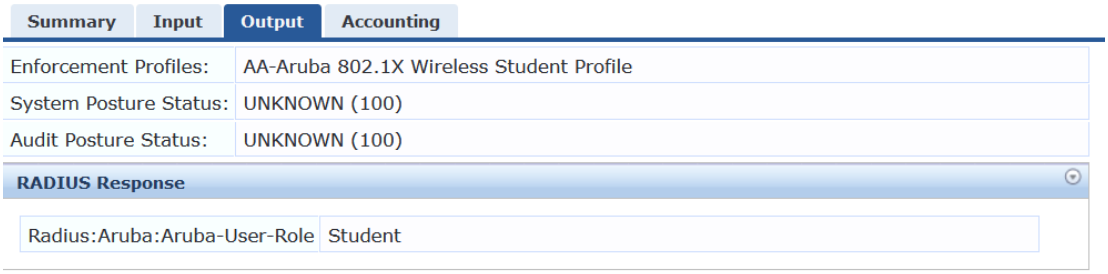
We’ll use the same win10 laptop connecting to the dot1x SSID. The username we are using is “test1” which is successfully authenticated. Note the Role that is matched in addition to “all-test-group-member”.



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

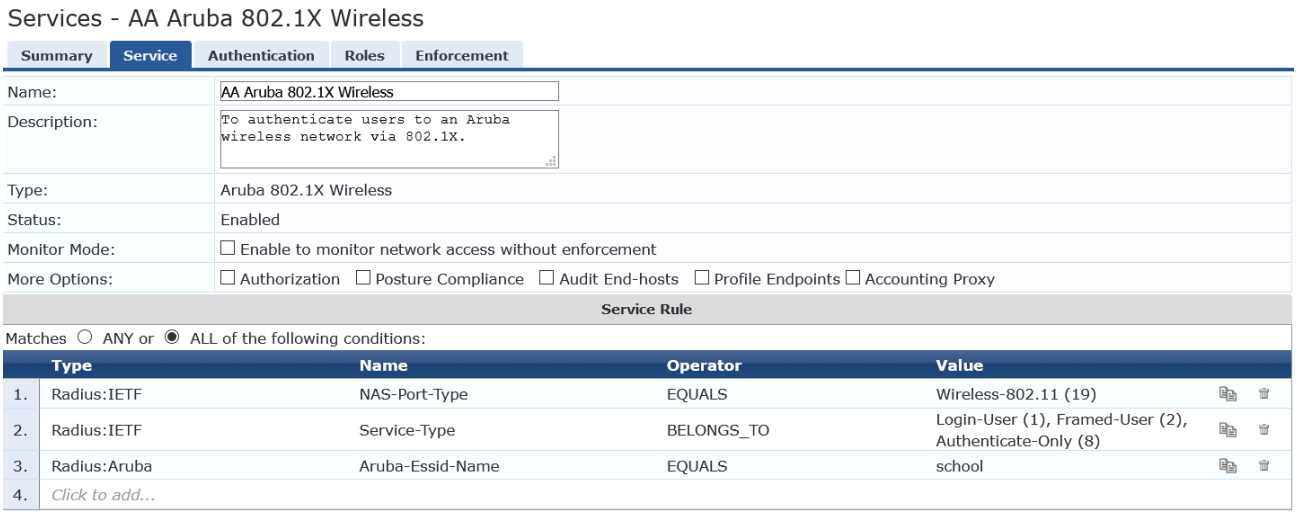


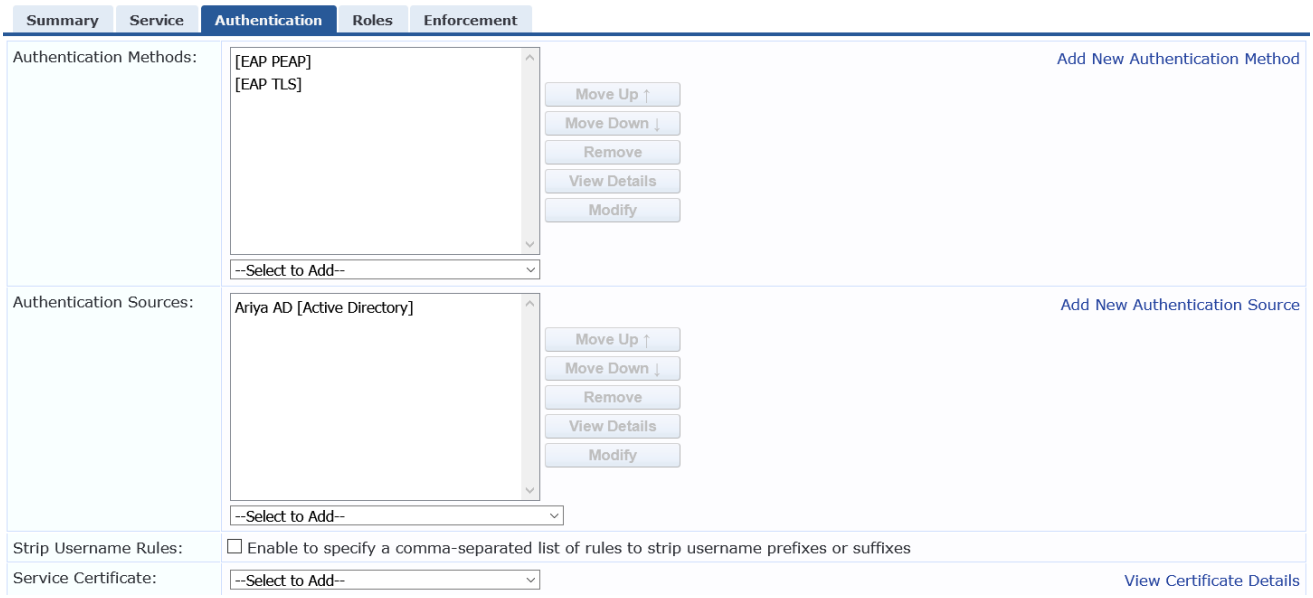
We also see the previous method's attribute values with red underline as shown above and finally the output tab that shows ClearPass sending back Aruba-user-role of Student.



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"

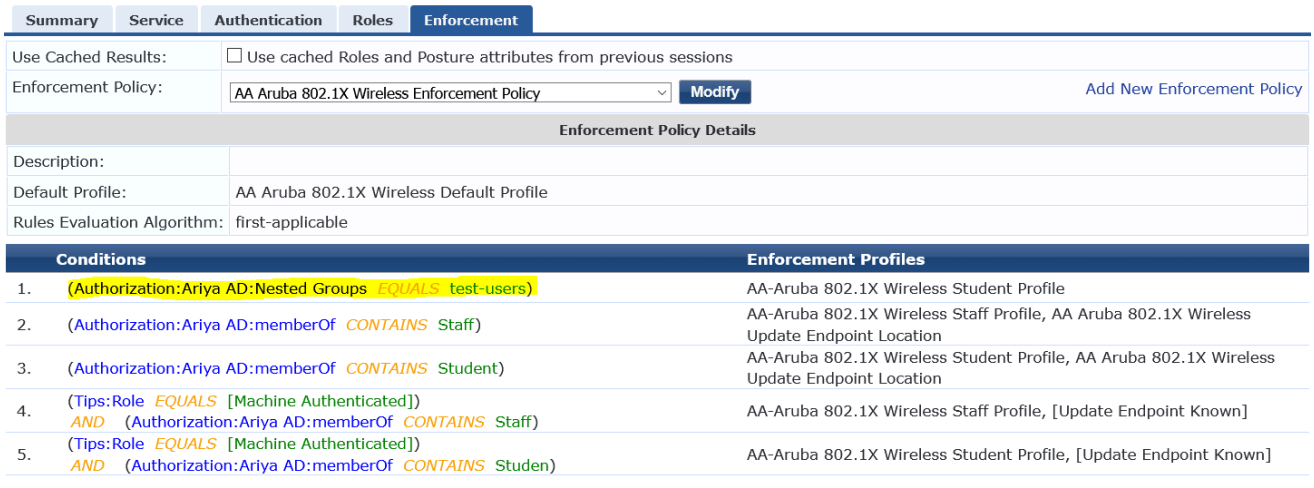
Here the modified dot1x service.



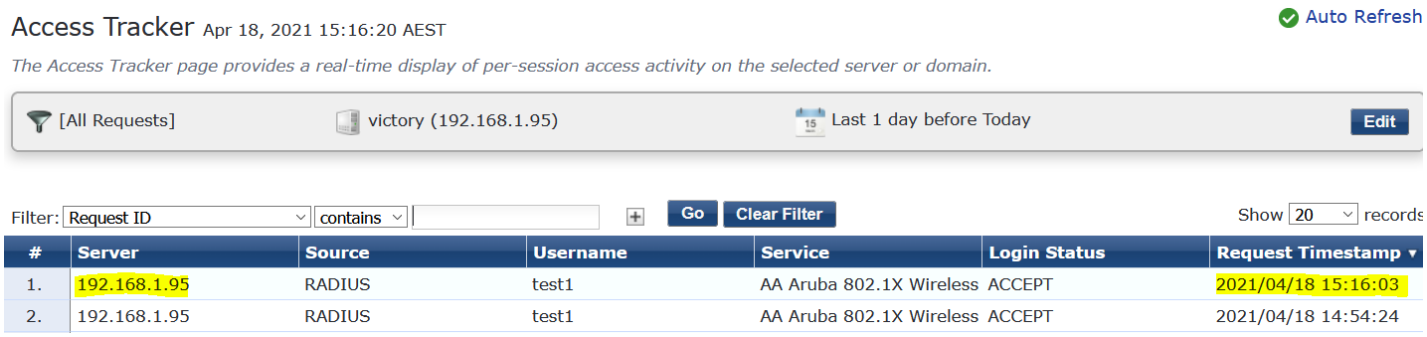


Note that here we have removed the role-mapping policy.

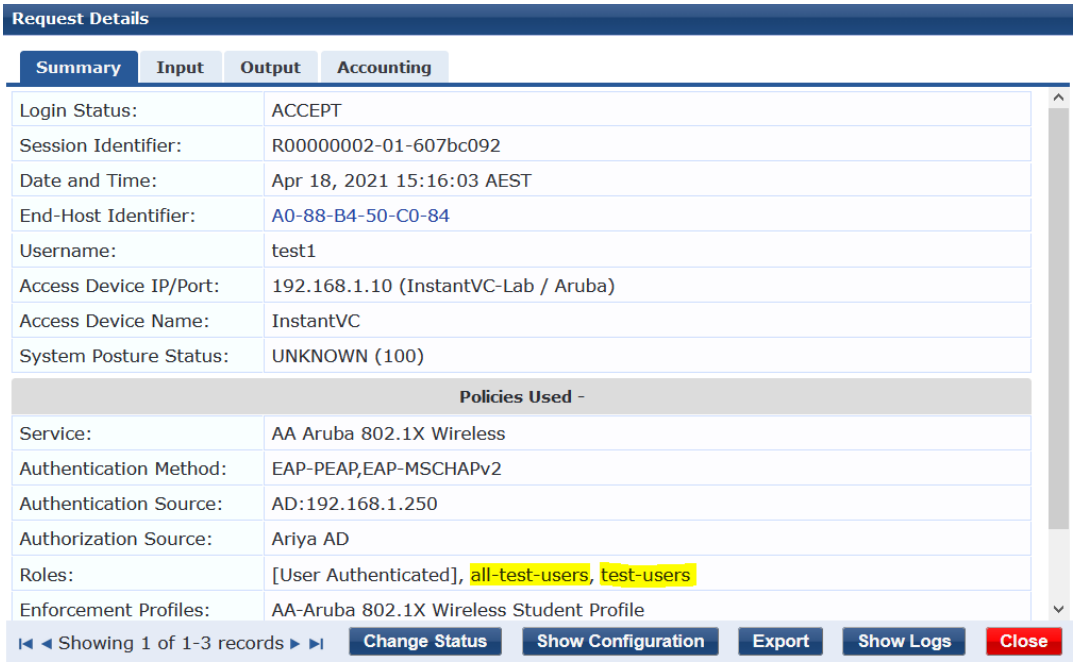
And here we have modified the first rule to check the new attribute “Nested Groups” which we added to the authentication source.



Now we’ll test again with the same username.

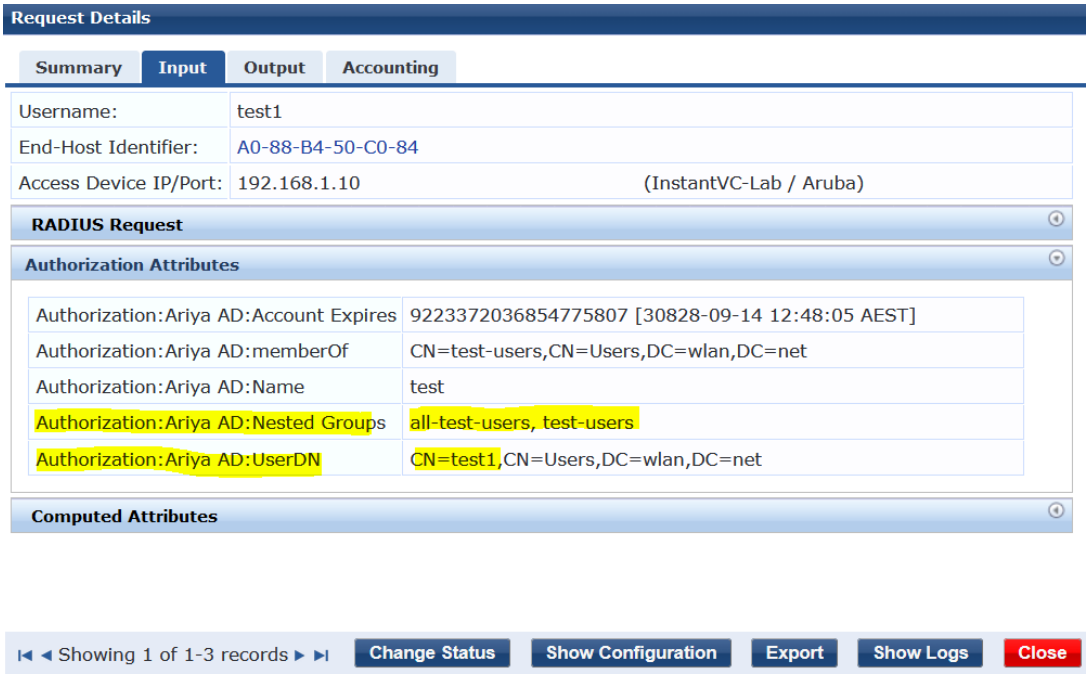


Checking the access tracker request



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



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