

Contents

1.1	Revision History	1
2	Nested AD group Configuration	2
2.1	Active Directory Groups	2
2.2	ClearPass Configuration	3
2.3	Testing	7
2.4	Modifying Enforcement policy	8

1.1 Revision History

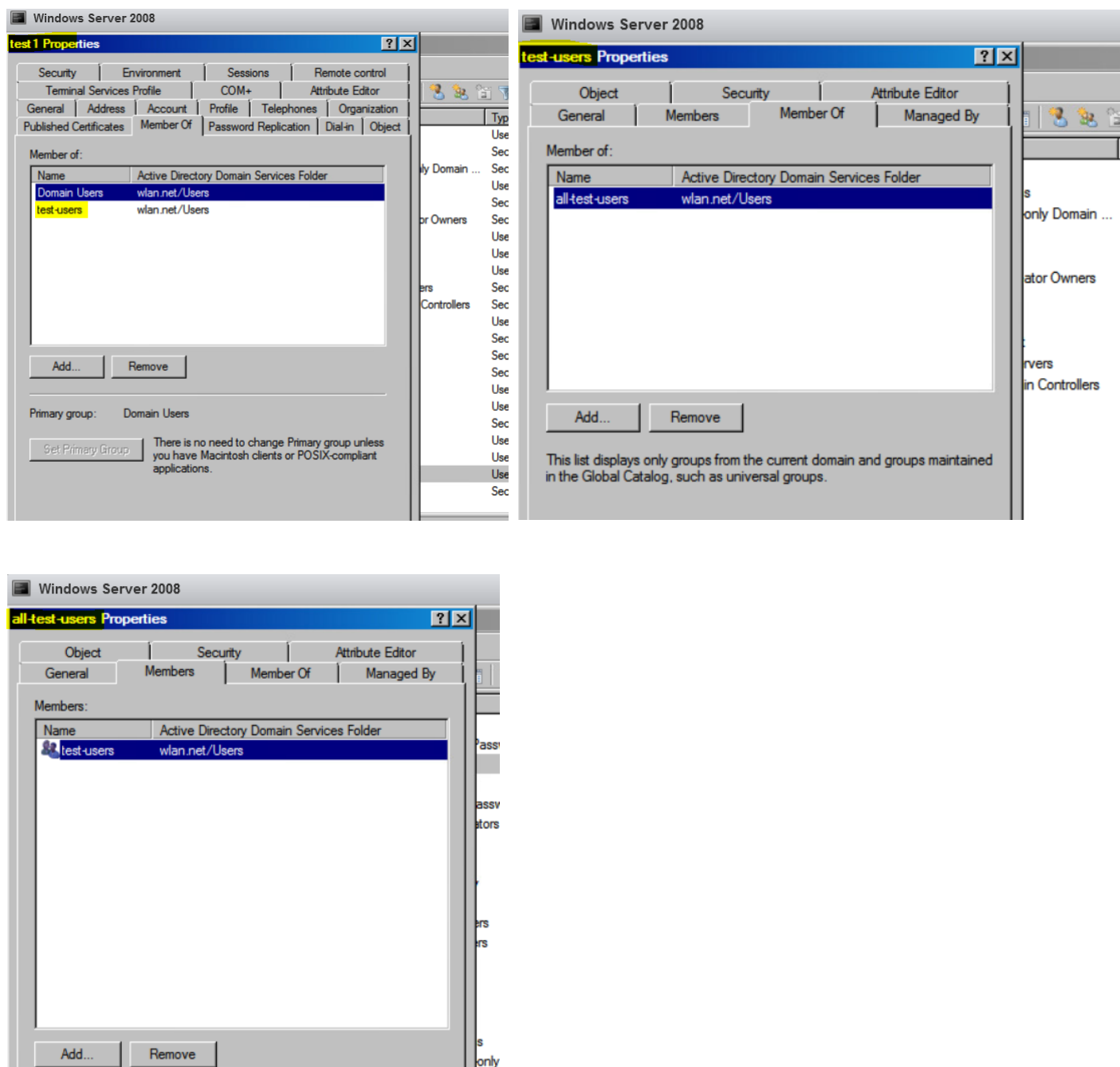
DATE	VERSION	EDITOR	CHANGES
02 Apr 2021	0.1	Ariya Parsamanesh	Initial creation

2 Nested AD group Configuration

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



ClearPass can check if test1 is a member of “test-users” but the condition will fail for checking membership of “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.

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains a navigation menu with categories: Dashboard, Monitoring, Configuration, Authentication, Identity, Posture, Enforcement, and Network. The 'Configuration' menu is expanded, showing 'Service Templates & Wizards', 'Services', 'Authentication', 'Methods', 'Sources', 'Identity', 'Single Sign-On (SSO)', 'Local Users', 'Endpoints', 'Static Host Lists', 'Roles', 'Role Mappings', 'Posture', 'Enforcement', 'Policies', 'Profiles', 'Network', 'Devices', 'Device Groups', 'Proxy Targets', 'Event Sources', and 'Network Scan'. The main content area is titled 'ClearPass Policy Manager' and shows the configuration for 'Authentication Sources - Ariya AD'. The 'Summary' tab is selected, displaying the following configuration details:

General:	
Name:	Ariya AD
Description:	
Type:	AD
Use for Authorization:	Enabled
Authorization Sources:	-

Primary:	
Hostname:	192.168.1.250
Connection Security:	None
Port:	389
Verify Server Certificate:	true
Bind DN:	administrator@wlan.net
Bind Password:	*****
NetBIOS Domain Name:	WLAN
Base DN:	dc=wlan,dc=net
Search Scope:	SubTree Search
LDAP Referrals:	false
Bind User:	true
User Certificate:	userCertificate

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

The screenshot shows the 'Attributes' tab for the 'Ariya AD' authentication source. The 'Attributes' tab is selected, displaying a table of attributes. The table has four columns: Filter Name, Attribute Name, Alias Name, and Enabled As. The table lists the following attributes:

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

An orange arrow points to the 'Group' filter name in the table. The 'Add More Filters' button is located at the bottom right of the table.

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".

Configure Filter

Configuration

Attributes

Browse

Filter

Filter Name: SubGroup
Filter Query: (distinguishedName={memberOf})

	Name	Alias Name	Data type	Enabled As	
1.	cn	SubGroups	String	-	
2.	memberOf	SubGroupmemberOf	String	<input type="checkbox"/> Role <input type="checkbox"/> Attribute	
3.	Click to add...				

Save

Close

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.

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	-

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.

Configure Filter

Configuration

Attributes

Browse

Filter

Filter Name: OneLevelUp
Filter Query: (distinguishedName={SubGroupmemberOf})

	Name	Alias Name	Data type	Enabled As	
1.	cn	OneLevelUp	String	-	
2.	memberOf	OneLevelUpmemberOf	String	-	
3.	Click to add...				

Save

Close

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”

The screenshot shows the Aruba ClearPass Policy Manager interface. On the left is a navigation menu with options like Dashboard, Monitoring, Configuration, Authentication, Identity, Posture, and Enforcement. The main area is titled 'ClearPass Policy Manager' and 'Configuration » Identity » Roles'. A modal window titled 'Edit Role' is open, showing the following details:

- Role ID: 3006
- Name: all-test-group-member
- Description: (empty text area)

At the bottom of the modal are 'Save' and 'Cancel' buttons.

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

The screenshot shows the Aruba ClearPass Policy Manager interface. The navigation menu is on the left. The main area is titled 'ClearPass Policy Manager' and 'Configuration » Identity » Role Mappings » Edit - nested-group'. The 'Role Mappings - nested-group' page has three tabs: 'Summary', 'Policy', and 'Mapping Rules'. The 'Policy' tab is selected, showing the following details:

- Policy Name: nested-group
- Description: (empty text area)
- Default Role: all-test-group-member

Below the policy details is the 'Mapping Rules' section. It shows 'Rules Evaluation Algorithm: First applicable'. A table lists the mapping rules:

Conditions	Role Name
1. (Authorization:Ariya AD:UpOneLevelmemberOf CONTAINS all-test-users)	all-test-group-member

aruba

ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Methods

Sources

Identity

Single Sign-On (SSO)

Local Users

Endpoints

Static Host Lists

Roles

Role Mappings

Configuration » Identity » Role Mappings » Edit - nested-group

Role Mappings - nested-group

Summary Policy Mapping Rules

Policy:

Policy Name: nested-group

Description:

Default Role: all-test-group-member

Mapping Rules:

Rules Evaluation Algorithm: First applicable

Conditions	Role Name
1. (Authorization:Ariya AD:OneLevelUpmemberOf CONTAINS all-test-users)	all-test-group-member

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.

Type: Aruba 802.1X Wireless

Status: Enabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

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

Summary Service Authentication Roles Enforcement

Authentication Methods:

[EAP PEAP]

[EAP TLS]

Move Up ↑

Move Down ↓

Remove

View Details

Modify

--Select to Add--

Add New Authentication Method

Authentication Sources:

Ariya AD [Active Directory]

Move Up ↑

Move Down ↓

Remove

View Details

Modify

--Select to Add--

Add New Authentication Source

Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Service Certificate: --Select to Add--

View Certificate Details

Summary Service Authentication Roles Enforcement

Role Mapping Policy: nested-group

Modify

Add New Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role: all-test-group-member

Rules Evaluation Algorithm: first-applicable

Conditions	Role
1. (Authorization:Ariya AD:UpOneLevelmemberOf CONTAINS all-test-users)	all-test-group-member

Summary	Service	Authentication	Roles	Enforcement
Use Cached Results:		<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions		
Enforcement Policy:		<div>AA Aruba 802.1X Wireless Enforcement Policy</div> <div>Modify</div>		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 Student)	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”

Request Details	
Summary	Input
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.

Request Details	
Summary	Input
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.

Access Tracker Apr 01, 2021 10:16:59 AEDT

Request Details

Summary Input **Output** Accounting

Enforcement Profiles: AA Aruba 802.1X Wireless Default Profile

System Posture Status: UNKNOWN (100)

Audit Posture Status: UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role Employee

Showing 1 of 1-5 records 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 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 Student)	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 Student)	AA-Aruba 802.1X Wireless Student Profile, [Update Endpoint Known]

Add Rule Copy Rule Move Up Move Down Edit Rule Remove Rule

Rules Editor

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value	
1.	Tips	Role	EQUALS	all-test-group-member	 
2.	Click to add...				

Enforcement Profiles

Profile Names:

[RADIUS] AA-Aruba 802.1X Wireless Student Profile

Move Up ↑

Move Down ↓

Remove

--Select to Add--

Save

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

Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches

Enforcement 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
3. (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

Back to Services

Copy

Save

Cancel

Services - AA Aruba 802.1X Wireless

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. (Tips:Role EQUALS all-test-group-member)	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
3. (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]

Back to Services

Disable

Copy

Save

Cancel

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

aruba ClearPass Policy Manager

Monitoring » Live Monitoring » Access Tracker

Access Tracker Apr 01, 2021 11:44:27 AEDT

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] victory (192.168.1.95) Last 1 day before Today

Filter: Request ID contains Go Clear Filter Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
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.

Request Details

Summary Input Output Accounting

Login Status: ACCEPT

Session Identifier: R00000002-01-60651744

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

Showing 1 of 1-8 records Change Status Show Configuration Export Show Logs Close

Request Details

Summary Input Output Accounting

Enforcement Profiles: AA-Aruba 802.1X Wireless Student Profile

System Posture Status: UNKNOWN (100)

Audit Posture Status: UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role Student

Showing 1 of 1-8 records Change Status Show Configuration Export Show Logs Close