

TECHNICAL NOTE

ClearPass and PSM RADIUS AUTHENTICATION

TABLE OF CONTENTS

	2
SETUP INSTRUCTIONS	2
ClearPass Setup	2
Import Pensando RADIUS dictionary	2
Create PSM device(s) and device group	3
Create enforcement profiles	4
Create the Roles and Role Mapping Policy	5
Create an Enforcement Policy	6
Create PSM Authentication Service	7
PSM Authentication Setup	10
Configure RADIUS Authentication Policy on PSM	10
Configure Role Binding on PSM	11
TEST THE AUTHENTICATION	12
Login into PSM using the RADIUS user	12
ClearPass Access Tracker Check	12
NEW USER ROLE	14
Create a new user group in PSM	14
Update Role Mapping Policy in ClearPass	15
Test the policy	17
USING PSM NAS-ID WITH CLEARPASS SERVICE DEFINITION	19
ADDITIONAL INFORMATION	20

Revision History

Document Version	Date	Prepared / Modified	Revisions
V1.0	09-Dec-2022	Gorazd Kikelj	Initial document
V1.1	10-Dec-2022	Gorazd Kikelj	Added PSM NAS-ID section



OVERVIEW

This document describes how to set up Aruba ClearPass RADIUS server for user authentication and authorization with AMD Pensando PSM (Policy and Services Manager).

SETUP INSTRUCTIONS

ClearPass Setup

To test the setup, you need a working ClearPass server. Installation and setup of Aruba ClearPass is not in the scope of this Technical Note.

Steps to setup the ClearPass environment for PSM:

- 1. Import Pensando RADIUS dictionary
- 2. Create PSM device and device group
- 3. Create Enforcement Profiles
- 4. Create Roles and Role Mapping Policy
- 5. Create Enforcement Policy
- 6. Create PSM Authorization Service

Import Pensando RADIUS dictionary

Cut & Paste the following xml definition into a file. After import the Pensando dictionary will be enabled by default. If this is not desirable, change value of the attribute "vendorEnabled" to "false".

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Wed Dec 07 12:07:22 CET 2022" version="6.10"/>
<Dictionaries>
<Vendor vendorEnabled="true" prefix="Pensando" name="Radius:Pensando" id="51886">
<RadiusAttributes>
<Attribute profile="in out" type="String" name="Pensando-User-Group" id="1"/>
<Attribute profile="in out" type="String" name="Pensando-Tenant" id="2"/>
</RadiusAttributes>
</Vendor>
</Dictionaries>
```

Navigate to the ClearPass GUI and import xml definition file into ClearPass dictionaries under Administration > Dictionaries > RADIUS. Click Import to perform the action.

Dashboard Administration = Oktionaries = RADIUS Monitoring RADIUS Dictionaries = RADIUS Monitoring This page allows admins to view the list of RADIUS dictionaries, view attributes and enable or export dictionaries. Administration This page allows admins to view the list of RADIUS dictionaries, view attributes and enable or export dictionaries. Administration Filter: [Vendor Name ▼ contains ▼] Go Clear Filter Show 20 ▼ records Administration Filter: [Vendor Name ▼ contains ▼] Go Clear Filter Show 20 ▼ records Administration Filter: [Vendor Name ▼ contains ▼] Go Clear Filter Show 20 ▼ records Administration I 3com false I 3com false false I Administration Administration false	aruba		Clear	Pass Policy Manager		Menu
Kontorring Carlos and privileges Administration Cleares and Privileges Second Privileges Administration Administratio	Dashboard O	Administration » Dictio	naries » RADIUS			
Configuration This page allows admins to view the list of RADIUS dictionaries, view attributes and enable or export dictionaries. Chain instruction Filter: Vendor Name V contains V Configuration Clear Filter Vendor 10 Vendor Prefix Enabled I. 3com Admin Users I. 3com I. 3com false I. 3com false I. 3com false	Monitoring O	RADIUS Diction	aries			🚊 Import
Administration Filter: Filter: Filter: Stort and Filter Stort and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Show 20 wreads • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Show 20 wreads • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Show 20 wreads • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter • Output and Filter	Configuration O	This name allows admir	is to view the list of RADIUS dictio	naries, view attributes and enable or export dictionaries		
ClearPass Portal Filter: [Vendor Name Contains Go Clear Filter Show 20 vecords Admin Users Admin Fivleges Vendor Name + Vendor ID Vendor Prefix Enabled Admin Source Admin Verges 1. 3com 43 3com false Admin Source 2. 3CPP 10415 3CPP false	Administration 📀	rns page anons aann		ands, then attributes and enable of export accontines.		
Publicers and Privileges Vendor Name	ClearPass Portal	Filter: Vendor Name	✓ contains ✓	Go Clear Filter		Show 20 🗸 records
Admin Users 1 3cm 43 3cm false admin Prilages 2 3GPP 10415 3GPP false advert Manager 3 Acc 1645 3GPP false	🖃 🖣 Users and Privileges	# Vendor Na	me	Vendor ID	Vendor Prefix	Enabled
Admin Privileges 2. 3GPP 10415 3GPP faise	- P Admin Users	1 3com		42	2 com	false
e 2 Server Manager 2. 3GPP 10415 3GPP 1186 → Reserver Manager Acc false	- Admin Privileges	I. Scom		43	acom	raise
Acc false	🖃 📶 Server Manager	2. 3GPP		10415	3GPP	false
Jimport from file	- P Server Configuration	3. Acc	Import from file		Acc	false
Acme false	- Jog Configuration	4. Acme			Acme	false
ADSL-Forum Select File: Izberite datoteko PensandoRasDictionary.xml ADSL-Forum false	- PLocal Shared Folders	5. ADSL-Forum	Select File:	Izberite datoteko PensandoRasDictionary.xml	ADSL-Forum	false
Adva Enter secret for the file (if any): Adva false	- J Licensing	6. Adva	Enter secret for the file (if any)	:	Adva	false
- Device Insight 7. Aerohive false false	- Povice Insight	7. Aerohive			Aerohive	false
External Servers 8. Airespace true	External Servers	8. Airespace			Airespace	true
External Accounts Alcatel Alcatel Alcatel faise	External Accounts Acceptificates	9 Alcatel			Alcatel	false
Acatel-Lucent-Enterprise true	Certificate Store	10. Alcatel-Luce			Alcatel-Lucent-Enterprise	true
Control of a service-Router false	- In Trust List	11. Alcatel-Luce			Alcatel-Lucent-Service-Router	false
Prevocation Lists 12 Altran	A Revocation Lists	12 Alteon			Altaon	false
Dictionaries	Dictionaries	12. Alceon			Alteon	false
Avaion raise	- 🎤 RADIUS	13. Alvarion			Alvarion	raise
PRADIUS Dynamic Authorization Tei 14. APC Taise	- PRADIUS Dynamic Authorization Ter	14. APC			APC	false
Arista Inport Cancel Arista Arista Arista	- PTACACS+ Services	15. Arista		Import Cancel	Arista	false
Povice Fingerprints 16. Arista-WiFi Arista-WiFi false	- JP Device Fingerprints	16. Arista-WiFi			Arista-WiFi	false
Dictionary Attributes 17. Aruba 14823 Aruba true	- PDictionary Attributes	17. Aruba		14823	Aruba	true
Applications 18. Ascend 529 Ascend false	- Applications	18. Ascend		529	Ascend	false
- D'Context Server Actions 19. Avenda 25427 Avenda true	- P Context Server Actions	19. Avenda		25427	Avenda	true
Dingress Events 20. Azaire 7751 Azaire false	- July Ingress Events	20. Azaire		7751	Azaire	false
A Windows Hotfixes	- Windows Hotfixes					
P Oncuard Custom scripts Showing 1/20 of 123 ₩ M	- OnGuard Custom Scripts	Showing 1-20 of 123 >	-			
end software updates	Agents and Software Updates					
P Undaria Setungs	# Software Undates					

Check the dictionary and enable it if needed for authentication to work.

Filter:	Vendor Name	✓ contains ✓ Per	sando 🕴	Go	Clear Filter				Show 20	✓ records
#	Vendor Na	ime ⊾		Vend	or ID		\	Vendor Prefix	Enabled	
1.	Pensando			51886	j		F	Pensando	true	
Showing	g 1-1 of 1	RADIUS Attributes					0			
		Vendor Name: # Attribute Name 1. Pensando-Tenant 2. Pensando-User-Grou	Pensando (51886)	1D 2 1	Type String String	I ii ii	n/Out n out n out			

Create PSM device(s) and device group

Under Configuration > Network > Devices add all PSM servers and respective RADIUS secrets.

Edit Device Details					8
Device SNMP Read Settings	SNMP Write Settings	CLI Settings	OnConnect Enfor	rcement	Attributes
Name:	PSM				
IP or Subnet Address:	(e.g., 192.168.1.10) or 192.168.1.1	/24 or 2001:db8:a	0b:12f0::	:1 or 2001:db8:a0b:12f0::1/64)
Device Groups:	PSM, ArubaOS CX	Environment			
Description:	Pensando Service	Manager	//		
RADIUS Shared Secret:	•••••		Verify:	•••••	••••
TACACS+ Shared Secret:			Verify:		
Vendor Name:	IETF	-			
Enable RADIUS Dynamic Authorizatio	n: 🗹 Port: 3799				
Enable RadSec:					
					Copy Save Cancel

Under Configuration > Network > Device Groups add a new group and add PSM servers into this group.

Edit Device Group							
		•					
Name:	PSM						
Description:	Pensando PSM cluster						
Format:	List 🗸						
NOTE: Only 20 v available and selected devices are shown. Use filter to see additional devices.							
Available Devices(47)	Selected Devices(1)						
	Filter Filter						
AP303-Central-AOS10 [10.0.0 MSR2024 [10.0.0.1]	0/8] PSM [10.100.0.34]						

Create enforcement profiles

Under **Configuration > Enforcement > Profiles** create enforcement profiles for users on PSM. Define as many as needed. Here is an example for a user in **admin-group**.

Profile:

Name:	PSM Admin User
Description:	PSM Admin User with role admin-role
Туре:	RADIUS
Action:	Accept
Device Group List:	1. PSM

Attributes:

	Туре	Name	Value
1.	Radius:Pensando	Pensando-Tenant =	default
2.	Radius:Pensando	Pensando-User-Group =	admin-group

To create a new profile, click on 🚽 Add link.

From drop down menu select RADIUS Based Enforcement.

Type the name of the profile and description text.

Leave Action on Accept. This is a default value.

Enforcement profile can be limited to one or more Device groups or can be available for all devices. In the example configuration the device group PSM is selected. IP addresses of PSMs are added to this group. This ensure that enforcement profile is used only when it is applied to devices in selected Device group.

Enforcement Profiles

Profile Attribute	es Summary
Template:	RADIUS Based Enforcement
Name:	PSM Admin User
Description:	PSM Admin User with role admin-role
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	PSM Remove
	View Details
	Modify
	Select V

Click Next and add Pensando RADIUS attributes. In the example Tenant is default and User Group is admin-group.

	Туре	Name		Value		
1.	Radius:Pensando	Pensando-Tenant	=	default	Ē	Ť
2.	Radius:Pensando	Pensando-User-Group	=	admin-group		Ť
з.	Click to add					

Click Save to save profile. Repeat the procedure for all Tenant / User-Groups in your environment.

Create the Roles and Role Mapping Policy

Create new roles for different type of PSM users under Configuration > Identity > Roles. Click + Add to add a new role.

Add New Role		8
Name:	PSM Admin	
Description:	PSM Administrator	
		Save Cancel

Use existing or add a new Role Mapping Policy to match the user to the role under **Configuration > Identity > Role Mappings**. Click **Add** to add a new policy. Enter the name of the new policy, description and default role. Default role is applied when there is no matching rule. In the example the role **[Other]** is used to prevent access for unauthorized users.

			PSM and	Clea	rPa	SS	RA	Tec JS /	hn Autl	ica nen	I N tica	ote tion	
Role M	appings												
Policy	Mapping Rules	Summary											
Policy Nam	ne:	PSM Users Mapping Policy											
Description	n:	Map users to PSM roles											
Default Ro	le:	[Other]	✓ View Details Modify										

Add Mapping Rules to match the users to respective PSM roles. In the example the **[Admin User Repository]** is used as authentication source. If user in **[Admin User Repository]** has a role of **Super Administrator** it will get a role of **PSM Admin**. Tailor your mapping policy to match your requirements.

Rule	s Editor					8		
	Conditions							
Mate	Matches ANY or O ALL of the following conditions:							
	Туре	Name	Operator	Value				
1.	Authorization: [Admin User Repository]	Role_Name	EQUALS	Super Administrator	E9	ŵ		
2.	Click to add							
			Actions					
Role	e Name: PSM Admin	~						
					Save	el		

The Role Mapping Policy will look like

Policy:

Policy Name:	PSM Users Mapping Policy
Description:	Map users to PSM roles
Default Role:	[Other]

Mapping Rules:

Rules Evaluation Algorithm:	First applicable	
Conditions	Role Nam	e
1. (Authorization: [Admin User Repository]: Role_Name EQUALS Super Administrator)	PSM Admir	1

Create an Enforcement Policy

Under **Configuration > Enforcement > Policy** create a new enforcement policy by clicking on **Add** button. Type the name of the policy, add description and select **Enforcement Type** as **RADIUS**. Select **[Deny Access Profile]** as default profile. Default profile is used when there is no matching conditions. For example, when Role Matching Policy return the role **[Other]**.

			Technical Note PSM and ClearPass RADIUS Authentication
Enforcemen	at Dalia	ice	
Enforcemen	IL POIL	les	
Enforcement	Rules	Summary	

Name:	PSM Enforcement Policy
Description:	Enforce PSM users
Enforcement Type:	● RADIUS \bigcirc TACACS+ \bigcirc WEBAUTH (SNMP/Agent/CLI/CoA) \bigcirc Application \bigcirc Event
Default Profile:	[Deny Access Profile] View Details Modify

Add Enforcement Policy Rules to map ClearPass roles to Pensando Enforcement profiles. In the example select **Tips** for **Type**, **Role** for **Name**, **EQUALS** for **Operator** and **PSM Admin** as the value. Select profile **PSM Admin User** as the **Enforcement Profile**. This rule will match when Mapping Policy returns role PSM Admin and it will perform an action defined in the enforcement profile **PSM Admin User**.

Rules Editor									
			Co	nditions					
Match ALL of the followi	ng conditions:								
Туре		Name		Operator		Value			_
1. Tips	•	Role	•	EQUALS	T	PSM Admin	•	Ð	ŵ
2. Click to add									
			Enforce	ment Profiles					
Profile Names:	[RADIUS] PSM A	dmin User							
			Move Up ↑						
			Move Down ↓						
			Remove						
	Select to Add			~					
							Save	Cance	el
							Ouro	Juno	

Enforcement:

Name:	PSM Enforcement Policy
Description:	Enforce PSM users
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm:	First applicable
Conditions	Actions
1. (Tips:Role EQUALS PSM Admin)	PSM Admin User

Create PSM Authentication Service

Create a new Service under Configuration > Services. In dropdown menu select RADIUS Enforcement (Generic). In the Service Rule select ALL of the following conditions. Add Service rules Connection > NAD-IP-Address > BELONGS_TO_GROUP > PSM (group you created for PSM servers), and Radius:IETF > NAD-Port-Type > EQUALS > Virtual (5).

aruba	ClearPass Policy Manager Menu 🗮						
Dashboard O	Configu	ration » Services »	Add				
🖌 Monitoring 🛛 🔍	Services						
Configuration 📀	Servic	e Authenticatio	Roles Enforcement Summary				
- 🛱 Service Templates & Wizards	Туре:		RADIUS Enforcement (Generic)				
Authentication	Name:		PSM Authentication				
- 🖨 Methods - 🏠 Sources	Descript	tion:	PSH RADIUS Authentication				
- Q Identity							
- 🛱 Single Sign-On (SSO)	Monitor	Mode:	Enable to monitor network access without enforcement				
- Q Local Users	More Op	ptions:	Authorization Posture Compliance Audit End-hosts Profile Endpoints Accounting Proxy				
- Grand Host Lists				Service Rule			
- C Roles	Matches	; 🔿 ANY or 💿 AI	L of the following conditions:				
Di Role Mappings		Туре	Name	Operator	Value		
🗈 📅 Posture	1.	Connection	NAD-IP-Address	BELONGS_TO_GROUP	PSM		
- 8 Enforcement	2.	Radius:IETF	NAS-Port-Type	EQUALS	Virtual (5)		
- 🛱 Policies	з.	Click to add					
- 🛱 Profiles							
Network							
- Q Devices							
- Device Groups							
Proxy Targets							
- Line Kimulatian							
- A Policy Simulation							
	d Rac	k to Services			Nort -> Savo Cancal		
Administration O	. 000	A 10 00 1003			HOAL CONCOL		

Click Next. Select Authentication Methods [PAP] and Authorization Source [Admin User Repository]. Click Next.

Configuration » Services » Add

Service	S				
Service	Authentication	Roles	Enforcement	Summary	
Authenticat	ion Methods:	[PAP]	Add		Move Up ↑ Move Down ↓ Remove View Details Modify
Authenticat	ion Sources:	[Admin Use	r Repository] [Loca Add	I SQL DB]	Move Up ↑ Move Down ↓ Remove View Details Modify
Strip Usern	ame Rules:	🗆 Enable t	o specify a comm	na-separated	list of rules to strip username prefixes or suffixes
Service Cer	tificate:	Select to /	Add	~	

Select Role Mapping Policy (PSM User Mapping Policy) created in previous steps. Click Next.

Technical Note

PSM and ClearPass RADIUS Authentication

Service	S							
Service	Authentication	Roles	Enforcement	Summary				
Role Mapping Policy:		PSM Users	Mapping Policy		✓ Modify			
Description:		Map users	Map users to PSM roles					
Default Ro	e:	[Other]						
Rules Evaluation Algorithm:		evaluate-a	II					
c	Conditions							
1. ((Authorization:[Admin User Repository]:Role_Name EQUALS Super Administrator)							

Select Enforcement Policy (PSM Enforcement Policy) created in previous steps. Click Save to save the Service.

Services - PSM Authentication

Summary	Service	Authentication	Roles	Enforcement	
Use Cached R	lesults:	Use cached F	Roles and	Posture attribute	s from previous sessions
Enforcement Policy: PSM Enforcement Policy			Modify		
					Enforcement Policy Details
Description:		Enforce PSM u	sers		
Default Profil	e:	[Deny Access	Profile]		
Rules Evaluat	tion Algorithr	n: first-applicable	9		
Cond	itions				Enforcement Profiles
1. (Tips	s:Role EQUA	LS PSM Admin)			PSM Admin User

Service is added to the end of the service list. Use Reorder button to move the service up.

Services This page shows the current list and order of services that ClearPass follows during authentication and authorization.					
Filter: Name v Contains v PSM + Go Clear	Filter	Hit Count for Last 1 hour 💌		Show 20 🗸 records	
# Order 🔺 Name	Туре	Template	Hit Count	Status	
1. C 4 PSM Authentication	RADIUS	RADIUS Enforcement (Generic)	0	0	
Showing 1-1 of 1			Reorder Copy	Export Delete	

Configuration » Services » Reorder

Reorder Services

To reorder services, first click on the service you want to move. Next, click on another service where you want to move the previously selected service:

Orde	r Name	*	Service Details:	
1	Authorization Services for Selectium		Name:	Authorization Services for Selectium
2	ALE Authentication Service		Template:	TACACS+ Enforcement
3	ArubaOS switch RADIUS mgmt login		Type:	TACACS
4	PSM Authentication		Description:	Authorisation services used to integrate authentication ac
5	ArubaOS-CX Radius Authorization		Status	Disabled
6	Demo - TACACS authorization and Enforcement		Status.	Disabled
7	Comware switch RADIUS mgmt login			Service Rule
8	AirWave Authorization Service		(Connection:Protocol E	QUALS TACACS)
9	ArubaOS controller login service			
10	API-Access OAuth2 API User Access			
11	iMC Authorization Service			
12	TAP-VPN Login Service			

Service Summary

Service:

Name:	PSM Authentication
Description:	PSM RADIUS Authentication
Туре:	RADIUS Enforcement (Generic)
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Ма	tch ALL of the following	conditions:		
	Туре	Name	Operator	Value
1.	Connection	NAD-IP-Address	BELONGS_TO_GROUP	PSM
2.	Radius:IETF	NAS-Port-Type	EQUALS	Virtual (5)

Authentication:

Authentication Methods:	[PAP]
Authentication Sources:	[Admin User Repository] [Local SQL DB]
Strip Username Rules:	-
Service Certificate:	-
Roles:	

Role Mapping Policy:	PSM Users Mapping Policy

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	PSM Enforcement Policy

ClearPass is now ready to accept authentication requests from PSM.

PSM Authentication Setup

Configure RADIUS Authentication Policy on PSM

Login to PSM. Go to Admin > Auth Policy and enable RADIUS. Add PSM server IP address into NAS ID. Add ClearPass IP address and RADIUS port (default is 1812) into Service Port. Add the same RADIUS secret used in Device registration on ClearPass into Server Secret field. Select PAP as Auth Method.

	Technical Note PSM and ClearPass RADIUS Authentication
Radius	SAVE CANCEL
CONFIG	
* NAS ID 10.100.0.34	
SERVER CONFIGURATION	+ ADD
* Server:Port 10.100.0.51:1812 * Server Secret	* Auth Method pap 🗸

NAS ID: IP address of the PSM server/cluster¹

Server:Port: IP/Port of the ClearPass server Server Secret: RADIUS secret used in ClearPass device registration Auth Method: PAP

Configure Role Binding on PSM

Go to Admin > User Management, select rolebinding from the top right pull down menu. By default, there is already a default AdminRoleBinding for admin privileges. Specify the group name defined in RADIUS Pensando-User-Group that can be mapped to this rolebinding. In this example, we use **admin-group** in our RADIUS attribute.

RBAC Managem	ent					
🚜 Manage	rolebin	ding				
Name: Role: User Groups:	AdminRoleBi AdminRole admin	nding e 🗸 -group 🗙				
Users:						
Availabl	le		Selected			
Search by name	Q	>	Search by name	Q		
	Gorazd	>>		admin		
		<		gorazd		
		~				
					Cancel	Save

¹ Check chapter USING PSM NAS-ID WITH CLEARPASS SERVICE DEFINITION for cluster deployments

TEST THE AUTHENTICATION

Login into PSM using the RADIUS user

Navigate to PSM login page and enter username from ClearPass [Admin User Repository].



Once successfully logged in, you will notice that dynamic user is being created on PSM with the correct role.

RBAC I	Management			
** N	lanage user			
Admin	Role (3)			
•f	Gorazd 🖪 Gorazd AdminRole		•	admin C Admin User AdminRole admin@selectium.local
•	gorazd (1) Gorazd Kikelj AdminRole gorazd.kikelj@selectium.c	om		

ClearPass Access Tracker Check

Check ClearPass Access tracker to see the authentication event.

Technical Note PSM and ClearPass RADIUS Authentication

3. cppm-selectium	RADIUS	Gorazd	PSM A	authentication	ACCEPT	
Request Details				8		
Summary Input O	utput					
Login Status:	ACCEPT			*		
Session Identifier:	R000069fe-23-63919b76					
Date and Time:	Dec 08, 2022 09:08:22 CET					
End-Host Identifier:	-					
Username:	Gorazd					
Access Device IP (Port):	10.100.0.34					
Access Device Name:	10.100.0.34 (PSM / IETF)					
System Posture Status:	UNKNOWN (100)					
	Policies Used -					
Service:	PSM Authentication					
Authentication Method:	PAP					
Authentication Source:	Local:localhost					
Authorization Source:	[Admin User Repository]					
Roles:	PSM Admin, [User Authenticated]					
Enforcement Profiles:	PSM Admin User			-		

Expand RADIUS Response in Output tab to see returned attributes.

Request Details		
Summary Input	Output	
Enforcement Profiles:	PSM Admin User	
System Posture Status:	UNKNOWN (100)	
Audit Posture Status:	UNKNOWN (100)	
RADIUS Response		
Radius:Pensando:Pens	ando-Tenant default	
Radius:Pensando:Pens	ando-User-Group admin-group	

NEW USER ROLE

Create a new user group in PSM

For new user group in PSM you need to create another role. In PSM GUI navigate to **User Management**. Select **role** at the top right pull down menu and select **Add Role**. This example create a role that can only read all the objects. Click **Save**.

RBAC Management		role 🗸 Refresh
🚢 Manage role		
Name: Audit Permissions: Configurations: Group: All V Kind: All V	Actions: All Actions Create Delete Read Update + AND	
		Cancel Save

Select **rolebinding** from the top right pull down menu. You should see that a new rolebinding object **Audit_binding** is created as the result of a new role **Audit** being created.



Click on the **Audit_binding** button and add a new User Group. In the example the group name is **audit-group**. Click **Save** to save the changes.

						PSM and	Te d ClearPass RADIUS	chnical N Authentica
RBAC Managem	ent						rolebinding \checkmark	Refresh
🚓 Manage	rolebing	ling						
Name: Role: User Groups:	Audit_bindin Audit v audit-	g group 🗙						
Users:								
Availab	le		Selected					
Search by name	Q Gorazd	> >>	Search by name	Q				
	admin	<						
	gorazd	~~						
					Cancel	Save		

Update Role Mapping Policy in ClearPass

You need to update Role Mapping Policy to map authentication parameters to ClearPass roles. Create a new role **PSM Audit** for PSM **audit-group** created in previous step.

Add New Role	8	
Name:	PSM Audit	
Description:	PSM Read Only All Objects	
	Save Cancel	

Add a new mapping rule in **PSM Users Mapping Policy**.

Technical Note

PSM and ClearPass RADIUS Authentication

Rule	s Editor				*
			Conditions		
Mate	ches $ullet$ ANY or $igloon$ ALL of the following condit	ions:			
	Туре	Name	Operator	Value	
1.	Authorization: [Admin User Repository]	Role_Name	EQUALS	Read-only Administrator	là t
2.	Click to add				
			Actions		
Role	e Name: PSM Audit	~			
					Save Cancel

Now you have two role mapping rules in the policy. User with **Super Administrator** role will have full Administrator access in PSM and user with **Read-only Administrator** role will have read only access in PSM.

Role	9 Mapping Rules:	
	Conditions	Role Name
1.	(Authorization:[Admin User Repository]:Role_Name EQUALS Super Administrator)	PSM Admin
2.	(Authorization:[Admin User Repository]:Role_Name EQUALS Read-only Administrator)	PSM Audit

Create ClearPass enforcement profile for audit-group.

Enforcement Profiles

Enforcement profile has not been saved

Profile	Attributes	Summary
vrofile:		
Template:		RADIUS B
Name:		PSM Audit
Description	1:	PSM Read
Type:		RADIUS
Action:		Accept
Device Gro	up List:	1. PSM

Attributes:

	Туре	Name		Value
1.	Radius:Pensando	Pensando-Tenant	=	default
2.	Radius:Pensando	Pensando-User-Group	=	audit-group

Add new rule to PSM Enforcement Policy

2. (Tips:R	ole EQUALS PSM Audit)	[RADIUS] PSM Audit User
------------	-----------------------	-------------------------

Enforcement Policies - PSM Enforcement Policy

Summary	Enforcement	Rules
Enforcement	:	
Name:	P	SM Enforc
Description:	E	nforce PSI
Enforcement	Type: R	ADIUS
Default Profile	e: [[Deny Acce

Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Actions
1.	(Tips:Role EQUALS PSM Admin)	PSM Admin User
2.	(Tips:Role EQUALS PSM Audit)	PSM Audit User

Test the policy

Login as the read only user.



In User Management you will see a new dynamic user psmAudit.



In ClearPass access tracker you will see new authorization request.

#	Server Name	Source	Username	Service	Login Status
1.	cppm-selectium	RADIUS	psmAudit	PSM Authentication	ACCEPT

In Output tab you can check RADIUS attributes sent to PSM.

Request Details						
Summary	Input	Output				
Enforcement	Profiles:	PSM Audit User				
System Posture Status:		UNKNOWN (100)				
Audit Posture Status:		UNKNOWN (100)				
RADIUS Res	ponse					
Radius:Pens	sando:Pens	sando-Tenant	default			
Radius:Pens	sando:Pens	sando-User-Group	audit-group			

USING PSM NAS-ID WITH CLEARPASS SERVICE DEFINITION

In standard production deployment the PSM operates as 3-node quorum-based cluster running on virtual machines (VMs) hosted on multiple servers for fault tolerance. Using PSM NAS-ID instead of IP addresses simplifies ClearPass RADIUS deployment.

Go to Auth Policy > Radius and edit NAS-ID parameter. In the example configuration NAS-ID value is PSM.

Radius					
CONFIG					
* NAS ID	PSM				

Change the ClearPass Service definition under **Configuration > Services** and use **Radius:IETF NAS-Identifier** instead of **Connection:NAD-IP-Address**.

Matches 🔿 ANY or 🖲 ALL of the following conditions:					
	Туре	Name	Operator	Value	
1.	Radius:IETF	NAS-Identifier	EQUALS	PSM	
2.	Radius:IETF	NAS-Port-Type	EQUALS	Virtual (5)	
з.	Click to add				

Check the RADIUS authentication request in Access Tracker. Radius:IETF:NAS-Identifier is now PSM instead of IP address.

Request Details			
	Summary Input	Output	
	Username:	Gorazd	
	End-Host Identifier:	-	
	Access Device IP (Port):	10.100.0.35	
	Access Device Name:	PSM (PSM1 / IETF)	
	RADIUS Request		
	Radius:IETF:NAS-Ident	itifier PSM	
	Radius:IETF:NAS-Port-	-Type 5	
	Radius:IETF:User-Nam	Gorazd	

ADDITIONAL INFORMATION

Additional information is available on asp.arubanetworks.com.



www.arubanetworks.com | info@arubanetworks.com

© Copyright Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.