

TECHNICAL NOTE

ClearPass and PSM

RADIUS AUTHENTICATION

TABLE OF CONTENTS

ClearPass and PSM.....	1
OVERVIEW	1
SETUP INSTRUCTIONS	1
ClearPass Setup.....	1
Import Pensando RADIUS dictionary	2
Create PSM device(s) and device group	3
Create enforcement profiles	3
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.....	10
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
ADDITIONAL INFORMATION	19

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

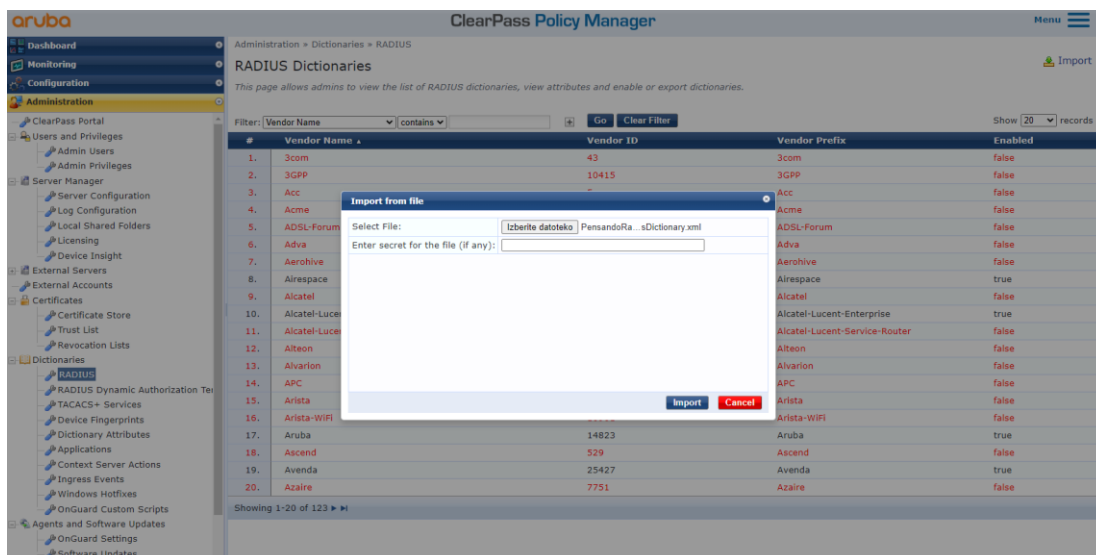
5. Create Enforcement Policy
6. Create PSM Authorization Service

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>
</TipsContents>
```

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



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

Filter: Vendor Name contains Pensando Go Clear Filter Show 20 records

#	Vendor Name	Vendor ID	Vendor Prefix	Enabled
1.	Pensando	51886	Pensando	true

Showing 1-1 of 1

RADIUS Attributes

Vendor Name: Pensando (51886)

#	Attribute Name	ID	Type	In/Out
1.	Pensando-Tenant	2	String	in out
2.	Pensando-User-Group	1	String	in out

Disable Export Close

Create PSM device(s) and device group

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

Edit Device Details

Device SNMP Read Settings SNMP Write Settings CLI Settings OnConnect Enforcement Attributes

Name: PSM

IP or Subnet Address: 10.100.0.34
(e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b: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 Authorization: ☒ 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 available and selected devices are shown. Use filter to see additional devices.

Available Devices(47) Filter

Selected Devices(1) Filter

AP303-Central-AOS10 [10.0.0.0/8]
MSR2024 [10.0.0.1]

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
Type:	RADIUS
Action:	Accept
Device Group List:	1. PSM

Attributes:

	Type	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
Attributes
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--

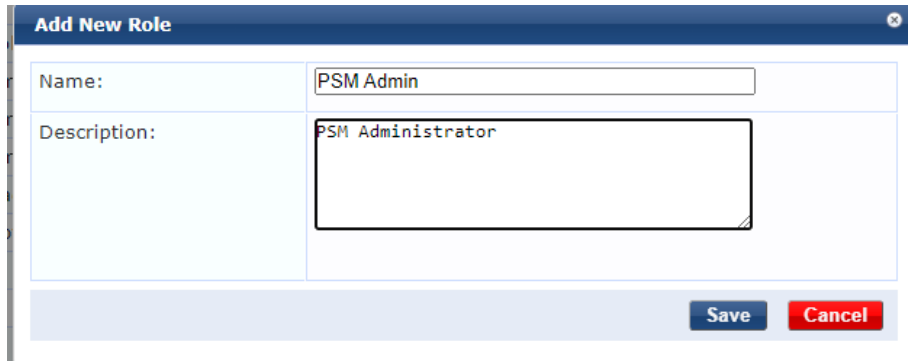
Click **Next** and add Pensando RADIUS attributes. In the example Tenant is **default** and User Group is **admin-group**.

Type	Name	Value		
1. Radius:Pensando	Pensando-Tenant	= default		
2. Radius:Pensando	Pensando-User-Group	= admin-group		
3. 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

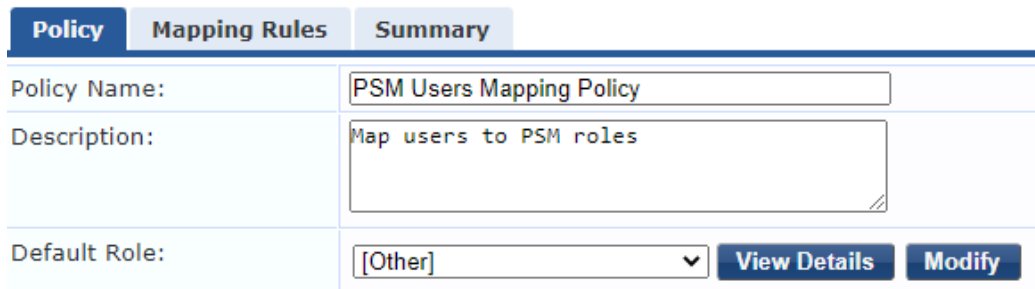
Name:


Description:

Save **Cancel**

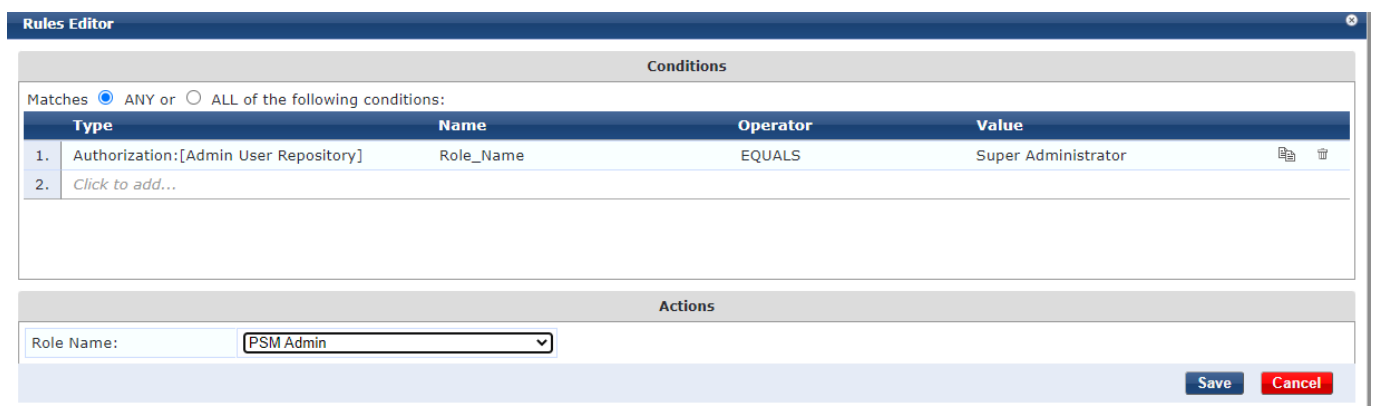
Use existing or add a new Role Mapping Policy to match the user to the role under **Configuration > Identity > Role Mappings**. Click  **Add** to add a new policy. Enter the name of the new policy, description and default role. Default role is applied when there is no matching rule. In the example the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

Role Mappings



Policy	Mapping Rules	Summary
Policy Name:	<input type="text" value="PSM Users Mapping Policy"/>	
Description:	<input type="text" value="Map users to PSM roles"/>	
Default Role:	<input type="text" value="[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.



Rules Editor

Matches ☒ ANY or ☐ ALL of the following conditions:

Type	Name	Operator	Value
1. Authorization:[Admin User Repository]	Role_Name	EQUALS	Super Administrator
2. Click to add...			

Actions

Role Name:

Save **Cancel**

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 Name
1. (Authorization:[Admin User Repository]:Role_Name EQUALS Super Administrator)	PSM Admin

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]**.

Enforcement Policies

Enforcement	Rules	Summary
<p>Name: PSM Enforcement Policy</p> <p>Description: Enforce PSM users</p> <p>Enforcement Type: <input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+ <input type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application <input type="radio"/> Event</p> <p>Default Profile: [Deny Access Profile] View Details Modify</p>		

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

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Tips	Role	EQUALS	PSM Admin
2. Click to add...			

Enforcement Profiles

Profile Names:

[RADIUS] PSM Admin User

Move Up ↑

Move Down ↓

Remove

--Select to Add--

Save

Cancel

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 <i>EQUALS</i> 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)**.

The screenshot shows the ClearPass Policy Manager web interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, Services, Identity, Posture, Enforcement, Network, and Administration. The main content area is titled 'Configuration > Services > Add' and shows the configuration for a new service named 'PSM Authentication'. The service type is 'RADIUS Enforcement (Generic)'. The description is 'PSM RADIUS Authentication'. The 'Monitor Mode' section has checkboxes for 'Enable to monitor network access without enforcement', 'Authorization', 'Posture Compliance', 'Audit End-hosts', 'Profile Endpoints', and 'Accounting Proxy'. The 'Service Rule' section shows a table with three conditions: 1. Connection, NAD-IP-Address, BELONGS_TO_GROUP, PSM; 2. Radius:IETF, NAS-Port-Type, EQUALS, Virtual (5); 3. Click to add... The bottom of the interface has buttons for 'Back to Services', 'Next', 'Save', and 'Cancel'.

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

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Authentication Methods:	<div> <div>[PAP]</div> <div> Move Up ↑ Move Down ↓ Remove View Details Modify </div> </div> <div>--Select to Add--</div>			
Authentication Sources:	<div> <div>[Admin User Repository] [Local SQL DB]</div> <div> Move Up ↑ Move Down ↓ Remove View Details Modify </div> </div> <div>--Select to Add--</div>			
Strip Username Rules:	<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes			
Service Certificate:	<div>--Select to Add--</div>			

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

Service	Authentication	Roles	Enforcement	Summary
Role Mapping Policy:	<div> <div>PSM Users Mapping Policy</div> <div>Modify</div> </div>			
Description:	Map users to PSM roles			
Default Role:	[Other]			
Rules Evaluation Algorithm:	evaluate-all			
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 Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	<div> <div>PSM Enforcement Policy</div> <div>Modify</div> </div>			
Enforcement Policy Details				
Description:	Enforce PSM users			
Default Profile:	[Deny Access Profile]			
Rules Evaluation Algorithm:	first-applicable			
Conditions			Enforcement Profiles	
1. (Tips:Role EQUALS PSM Admin)			PSM Admin User	

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

Services

+ Add
Import
Export All

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: <input type="text" value="Name"/>		<input type="text" value="contains"/>	<input type="text" value="PSM"/>	<input type="button" value="Go"/>	<input type="button" value="Clear Filter"/>	Hit Count for <input type="text" value="Last 1 hour"/>		Show <input type="text" value="20"/> records
#	<input type="checkbox"/>	Order ▲	Name	Type	Template	Hit Count	Status	
1.	<input type="checkbox"/>	4	PSM Authentication	RADIUS	RADIUS Enforcement (Generic)	0		
Showing 1-1 of 1								
<div><input type="button" value="Reorder"/><input type="button" value="Copy"/><input type="button" value="Export"/><input type="button" value="Delete"/></div>								

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:

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

Service Summary

Service:

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

Service Rule

Match ALL of the following conditions:

	Type	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**.

NAS ID: IP address of the PSM server/cluster

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 Management



Manage rolebinding

Name:

AdminRoleBinding

Role:

AdminRole ▾

User Groups:

admin-group ✕

Users:

Available

Search by name 🔍

Gorazd

>

>>

<

<<

Selected

Search by name 🔍

admin

gorazd

Cancel

Save

11

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 Management

Manage user

AdminRole (3)

 Gorazd  Gorazd AdminRole	 admin  Admin User AdminRole admin@selectium.local
 gorazd  Gorazd Kikelj AdminRole gorazd.kikelj@selectium.com	

ClearPass Access Tracker Check

Check ClearPass Access tracker to see the authentication event.

3.	cpm-selectium	RADIUS	Gorazd	PSM Authentication	ACCEPT
----	---------------	--------	--------	--------------------	--------

Request Details

Summary Input Output

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

◀ Showing 3 of 1-20 records ▶
 Change Status Show Configuration Export Show Logs Close

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:Pensando-Tenant	default
Radius:Pensando:Pensando-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 Add Role

Name:

Permissions:

Configurations:	Actions:
Group: <input type="text" value="All"/>	<input type="checkbox"/> All Actions
Kind: <input type="text" value="All"/>	<input type="checkbox"/> Create
	<input type="checkbox"/> Delete
	<input checked="" type="checkbox"/> Read
	<input type="checkbox"/> 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.

RBAC Management rolebinding ▾ Refresh

Manage rolebinding Add Rolebinding

AdminRoleBinding Created: 11/29/2022 10:16 AM Role: AdminRole <input type="text" value="admin"/> <input type="text" value="gorazd"/>	Audit_binding Created: 12/08/2022 11:26 AM Role: Audit
--	---

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.

RBAC Management
rolebinding ▼
Refresh

Manage rolebinding
Add Rolebinding

Name: Audit_binding
Role: Audit ▼
User Groups: audit-group X
Users:

Available
Search by name
Gorazd
admin
gorazd

>
>>
<
<<

Selected
Search by name

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

Name: PSM Audit
Description: PSM Read Only All Objects

Save
Cancel

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

Rules Editor

Conditions

Matches ☒ ANY or ☐ ALL of the following conditions:

	Type	Name	Operator	Value	
1.	Authorization:[Admin User Repository]	Role_Name	EQUALS	Read-only Administrator	
2.	Click to add...				

Actions

Role Name: PSM Audit

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 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

Profile:

Template:	RADIUS Based Enforcement
Name:	PSM Audit User
Description:	PSM Read Only Access to all objects
Type:	RADIUS
Action:	Accept
Device Group List:	1. PSM

Attributes:

	Type	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:Role EQUALS PSM Audit)	[RADIUS] PSM Audit User
----	------------------------------	-------------------------

Enforcement Policies - PSM Enforcement Policy

Summary Enforcement Rules

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
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.

Manage user

AdminRole (3)

Gorazd
Gorazd
AdminRole

gorazd
Gorazd Kikelj
AdminRole
gorazd.kikelj@selectium.com

psmAudit
psmAudit
Audit

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
Enforcement Profiles:	PSM Audit User
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)
RADIUS Response	
Radius:Pensando:Pensando-Tenant	default
Radius:Pensando:Pensando-User-Group	audit-group

ADDITIONAL INFORMATION

Additional information is available on asp.arubanetworks.com.