

## TECHNICAL NOTE

# ClearPass and PSM

## RADIUS AUTHENTICATION

## TABLE OF CONTENTS

OVERVIEW .....	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:

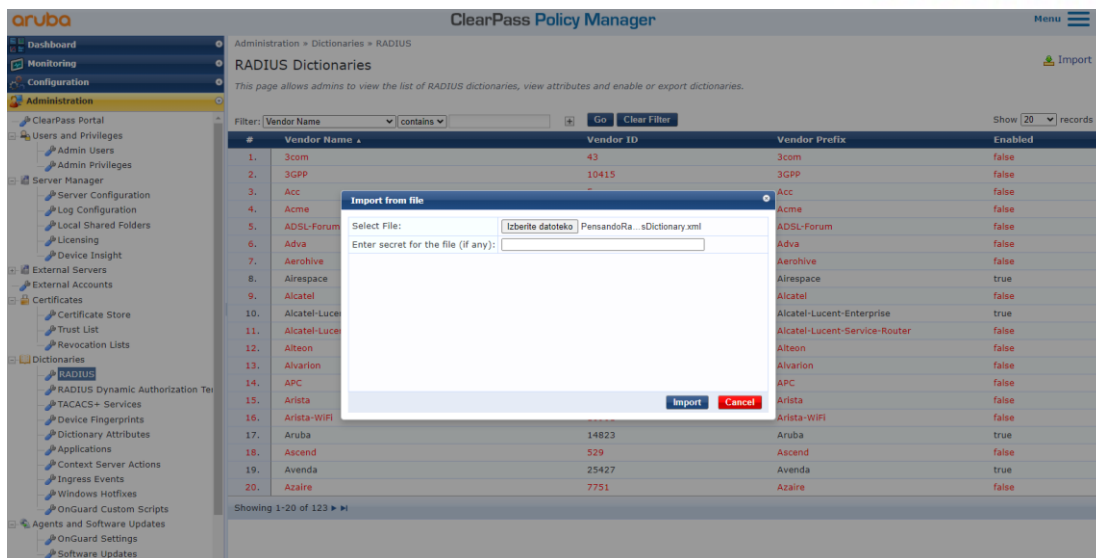
1. Import Pensando RADIUS dictionary
2. Create PSM device and device group
3. Create Enforcement Profiles
4. Create Roles and Role Mapping Policy
5. Create Enforcement Policy
6. Create PSM Authorization Service

### Import Pensando RADIUS dictionary

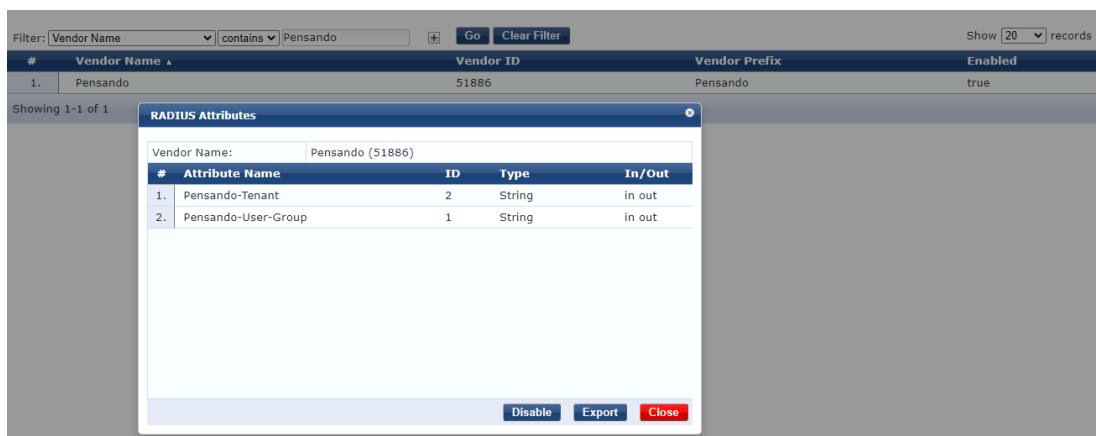
Cut & Paste the following xml definition into a file. After import the Pensando dictionary will be enabled by default. If this is not desirable, change value of the attribute "vendorEnabled" to "false".

```
<?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>
</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.



## 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
<p>Name: PSM</p> <p>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)</p> <p>Device Groups: PSM, ArubaOS CX Environment</p> <p>Description: Pensando Service Manager</p> <p>RADIUS Shared Secret: ***** Verify: *****</p> <p>TACACS+ Shared Secret: Verify:</p> <p>Vendor Name: IETF</p> <p>Enable RADIUS Dynamic Authorization: <input checked="" type="checkbox"/> Port: 3799</p> <p>Enable RadSec: <input type="checkbox"/></p>					
<p>Copy Save Cancel</p>					

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

**Edit Device Group**

Name:	<input type="text" value="PSM"/>
Description:	<input type="text" value="Pensando PSM cluster"/>
Format:	<input type="text" value="List"/>

**NOTE:** Only  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:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<div> <div>PSM</div> <div>Remove</div> <div>View Details</div> <div>Modify</div> </div> <div>--Select-- ▼</div>	

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:

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.

## Role Mappings

Policy	Mapping Rules	Summary
Policy Name:	PSM Users Mapping Policy	
Description:	Map users to PSM roles	
Default Role:	[Other] ▼	<a href="#">View Details</a> <a href="#">Modify</a>

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				
Conditions				
Matches <input checked="" type="radio"/> ANY or <input type="radio"/> 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:	PSM Admin ▼			
				<a href="#">Save</a> <a href="#">Cancel</a>

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
Name:	PSM Enforcement Policy	
Description:	Enforce PSM users	
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	
Default Profile:	<div>[Deny Access Profile] View Details Modify</div>	

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 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)**.

Configuration » Services » Add

Services

Service Authentication Roles Enforcement Summary

Type:

Name:

Description:

Monitor Mode: ☐ Enable to monitor network access without enforcement

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

Matches ☐ ANY or ☒ 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)
3. Click to add...			

Back to Services

Next Save 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:

[PAP]

Move Up ↑

Move Down ↓

Remove

View Details

Modify

--Select to Add--

Authentication Sources:

[Admin User Repository] [Local SQL DB]

Move Up ↑

Move Down ↓

Remove

View Details

Modify

--Select to Add--

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

Service Certificate: --Select to Add--

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



## Services

Service	Authentication	Roles	Enforcement	Summary
Role Mapping Policy: <span>PSM Users Mapping Policy</span> <span>Modify</span>				
Description: Map users to PSM roles				
Default Role: [Other]				
Rules Evaluation Algorithm: evaluate-all				
<b>Conditions</b>				
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: <span>PSM Enforcement Policy</span> <span>Modify</span>				
<b>Enforcement Policy Details</b>				
Description: Enforce PSM users				
Default Profile: [Deny Access Profile]				
Rules Evaluation Algorithm: first-applicable				
<b>Conditions</b>				
1. (Tips:Role EQUALS PSM Admin)				
<b>Enforcement Profiles</b>				
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:  contains

Hit Count for

Show  records

#	<input type="checkbox"/>	Order <span>▲</span>	Name	Type	Template	Hit Count	Status
1.	<input type="checkbox"/>	4	PSM Authentication	RADIUS	RADIUS Enforcement ( Generic )	0	

Showing 1-1 of 1

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 -----	Name: ----- Authorization Services for Selectium ----- Template: TACACS+ Enforcement Type: TACACS Description: Authorisation services used to integrate authentication ac Status: Disabled
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	<b>Service Rule</b> (Connection:Protocol EQUALS TACACS)
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**.

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/cluster<sup>1</sup>

**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

<sup>1</sup> Check chapter USING PSM NAS-ID WITH CLEARPASS SERVICE DEFINITION for cluster deployments

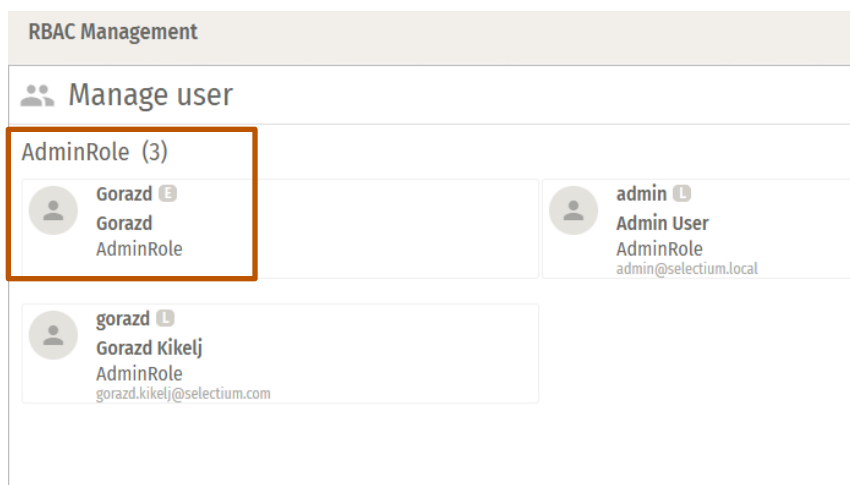
## TEST THE AUTHENTICATION

### 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.



### ClearPass Access Tracker Check

Check ClearPass Access tracker to see the authentication event.

3.	cppm-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:

Group:  ▾

Kind:  ▾

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.

RBAC Management rolebinding ▾ Refresh

**Manage rolebinding** Add Rolebinding

**AdminRoleBinding**  
Created: 11/29/2022 10:16 AM  
Role: AdminRole

**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

## 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:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Identifier	EQUALS	PSM
2. Radius:IETF	NAS-Port-Type	EQUALS	Virtual (5)
3. <a href="#">Click to add...</a>			

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

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

## ADDITIONAL INFORMATION

Additional information is available on [asp.arubanetworks.com](http://asp.arubanetworks.com).