TECHNICAL NOTE

# ClearPass and PSM

## RADIUS AUTHENTICATION

## TABLE OF CONTENTS



## 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:

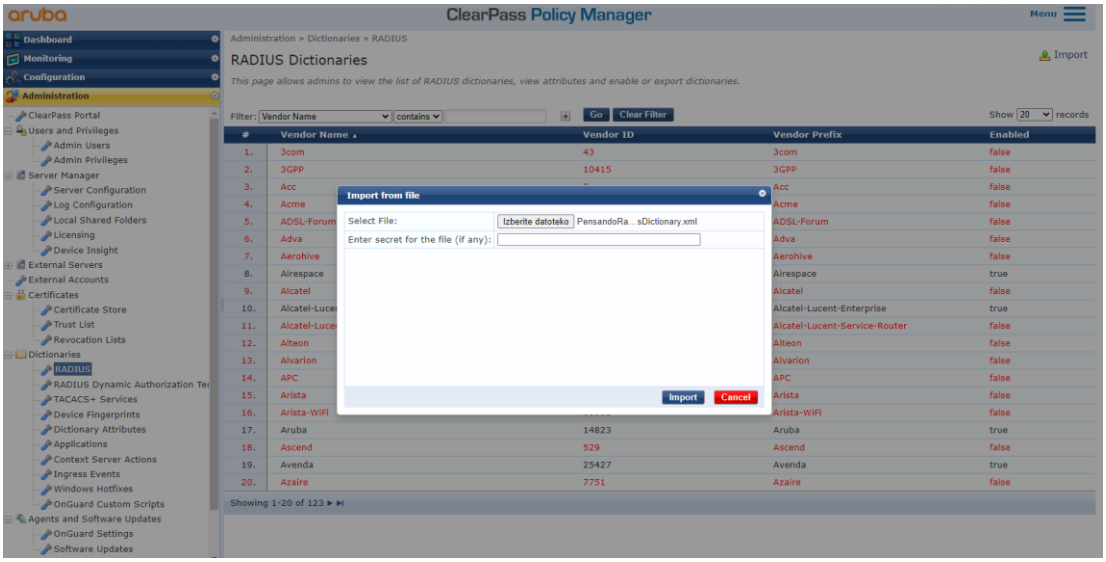
1. Import Pensando RADIUS dictionary
2. Create PSM device and device group
3. Create Enforcement Profiles
4. Create Roles and Role Mapping Policy
5. Create Enforcement Policy
6. Create PSM Authorization Service

### Import Pensando RADIUS dictionary

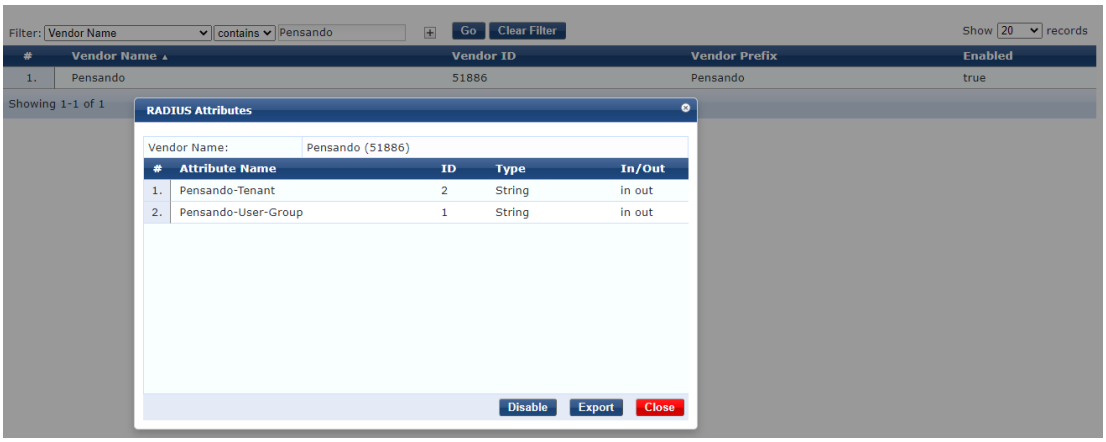
Cut & Paste the following xml definition into a file. After import the Pensando dictionary will be enabled by default. If this is not desirable, change value of the attribute “vendorEnabled” to “false”.

```
<?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.

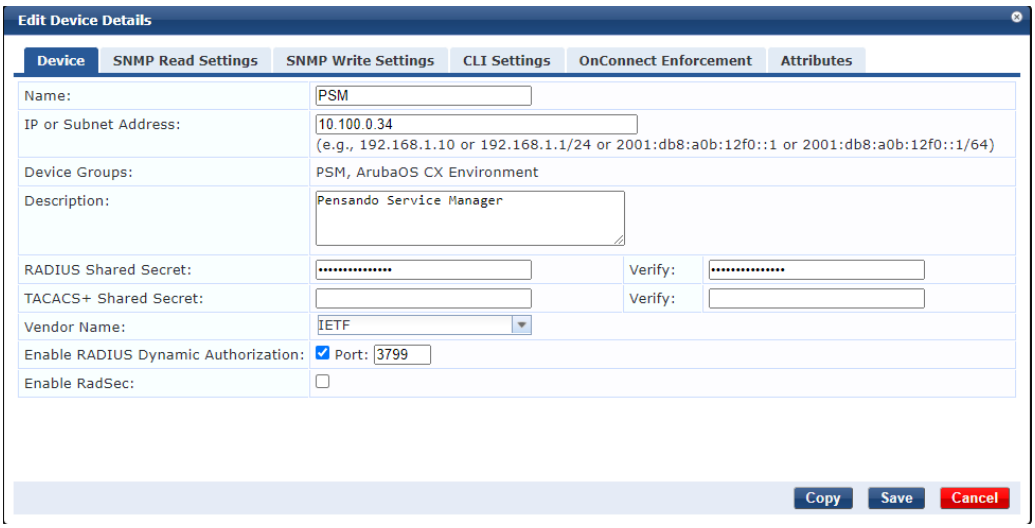



Check the dictionary and enable it if needed for authentication to work.

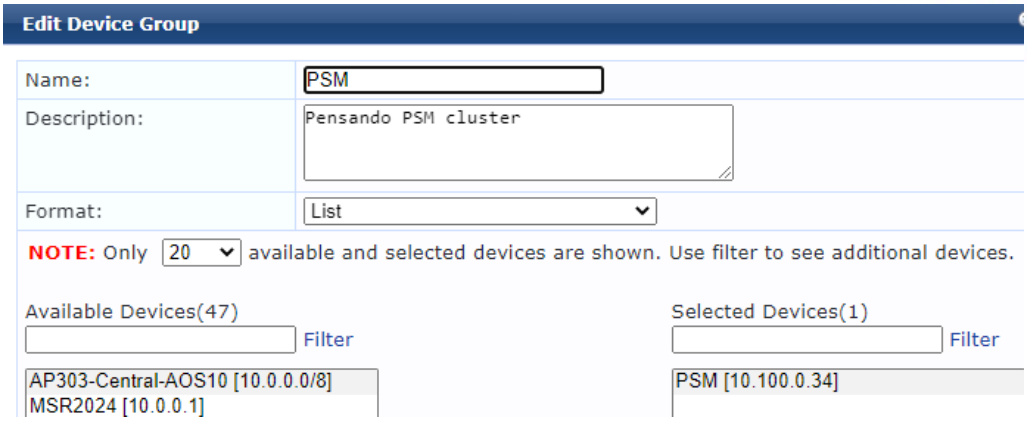



## Create PSM device(s) and device group

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




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




## 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 |

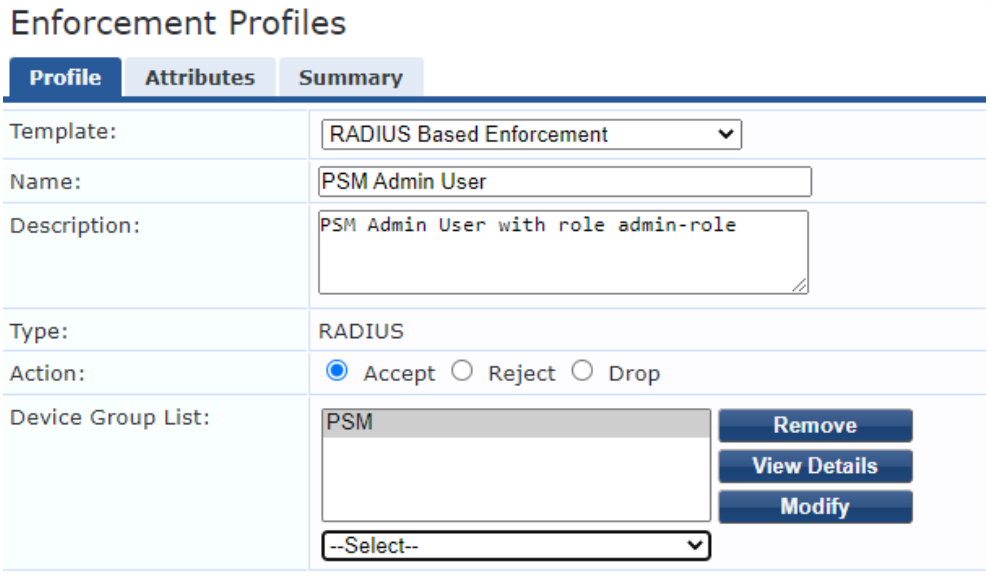
To create a new profile, click on Add link.

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.

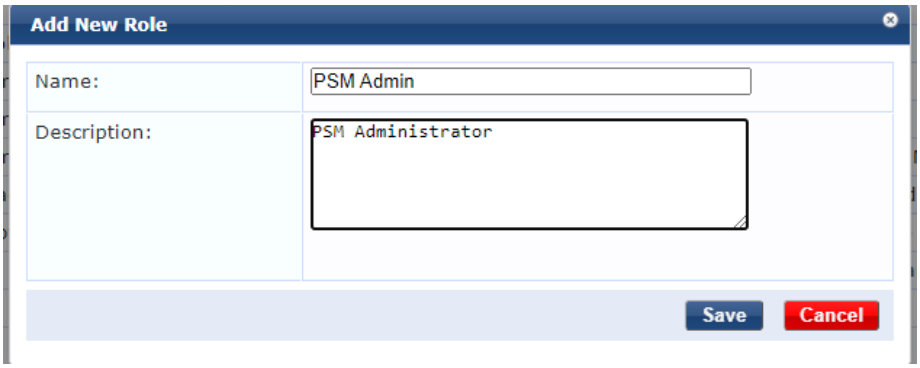



Click **Next** and add Pensando RADIUS attributes. In the example Tenant is **default** and User Group is **admin-group**.

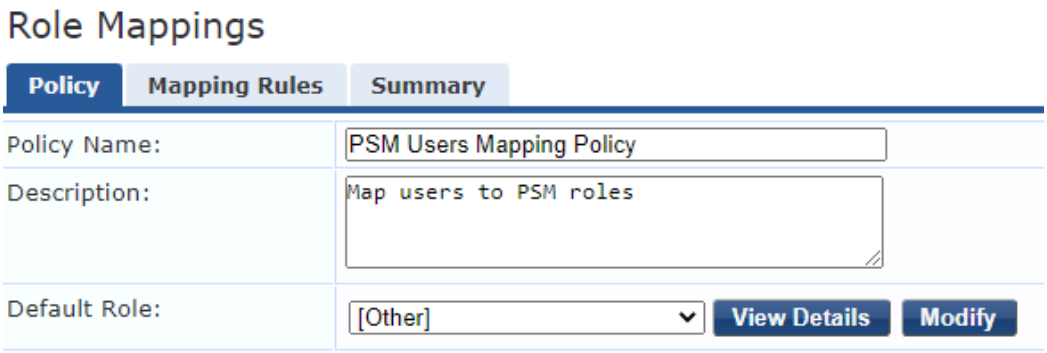

Click **Save** to save profile. Repeat the procedure for all Tenant / User-Groups in your environment.

## Create the Roles and Role Mapping Policy

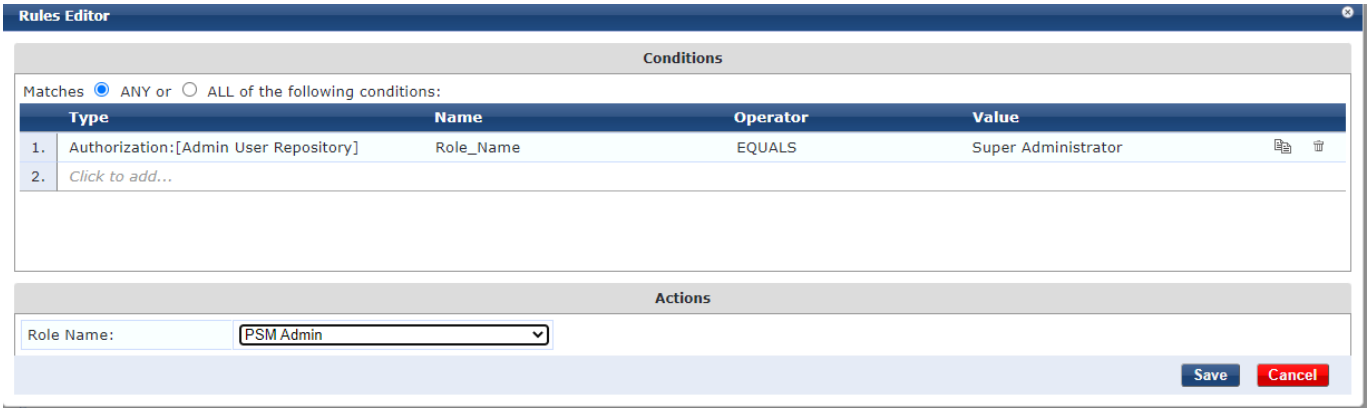
Create new roles for different type of PSM users under **Configuration > Identity > Roles**. Click Add to add a new role.




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.




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.




The Role Mapping Policy will look like

**Policy:**

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

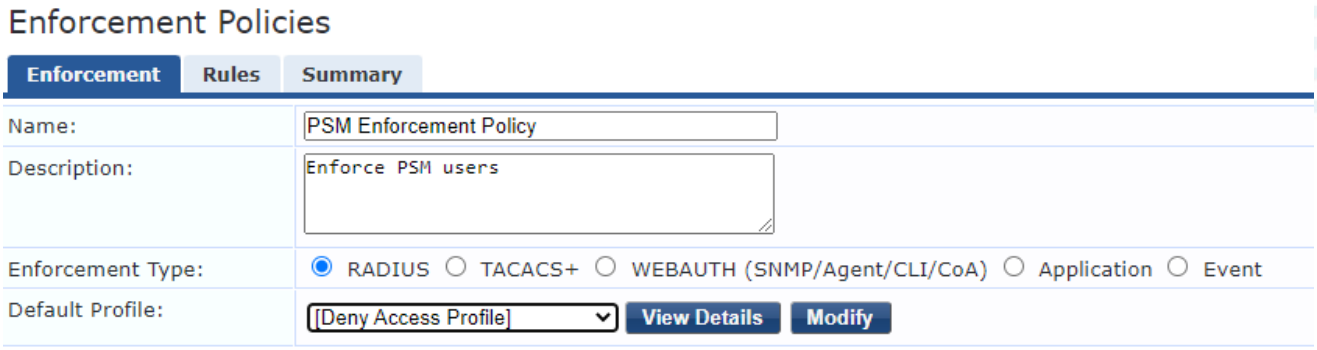
**Mapping Rules:**

| Rules Evaluation Algorithm: | First applicable |
|---|---|

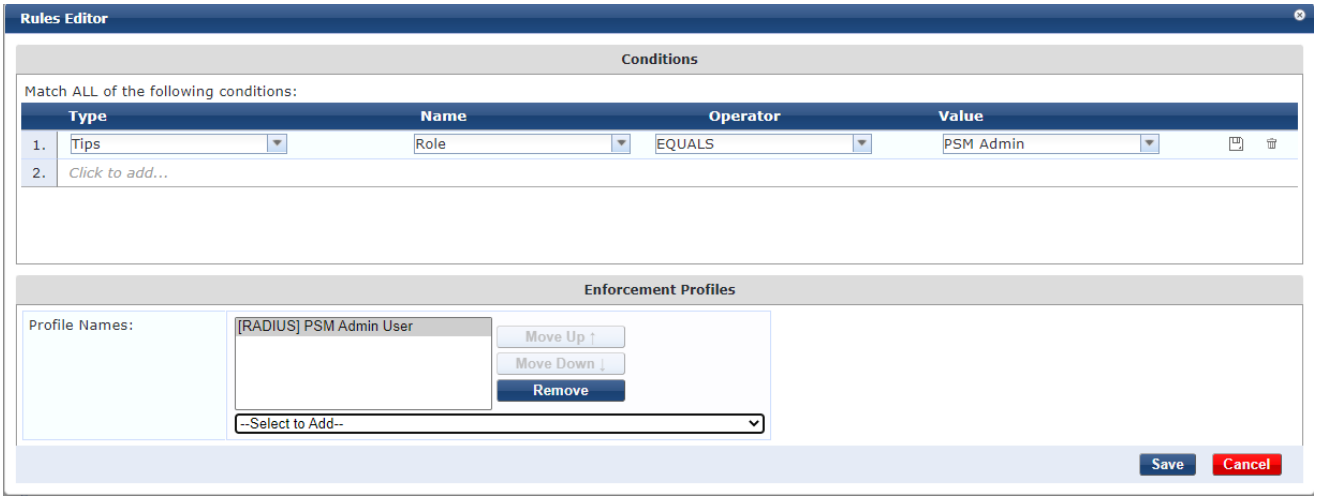
| | Conditions | Role Name |
|---|---|---|
| 1. | (Authorization:[Admin User Repository]:Role_Name *EQUALS* Super Administrator) | PSM Admin |

## 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]**.




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**.




## Enforcement:

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

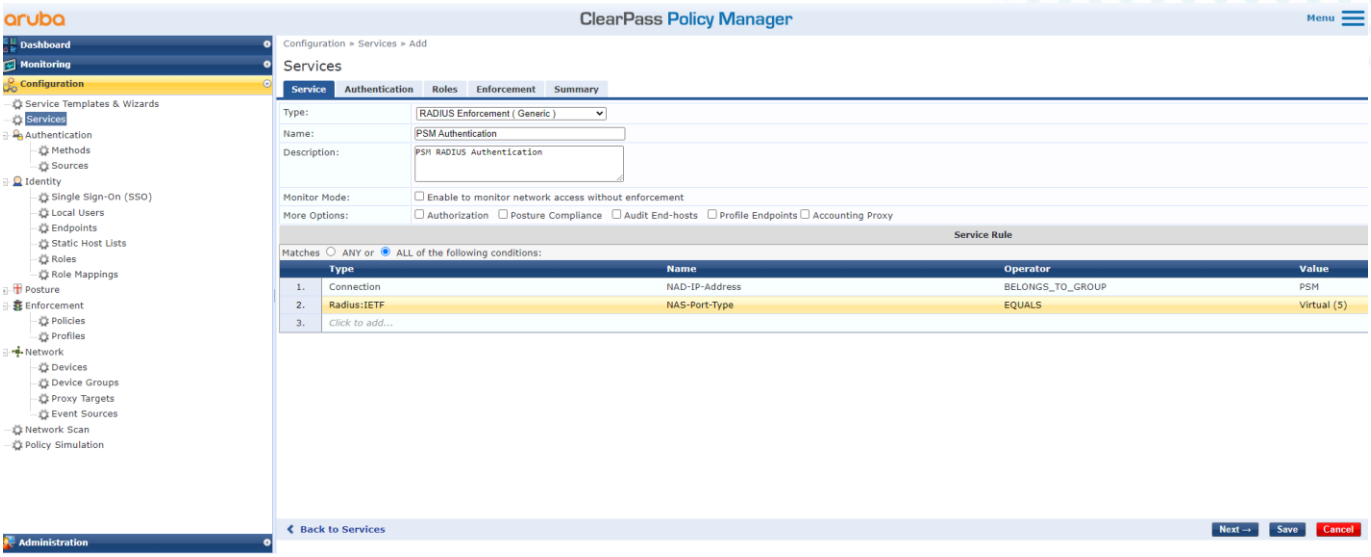
## Rules:

| | |
|---|---|
| Rules Evaluation Algorithm: | First applicable |

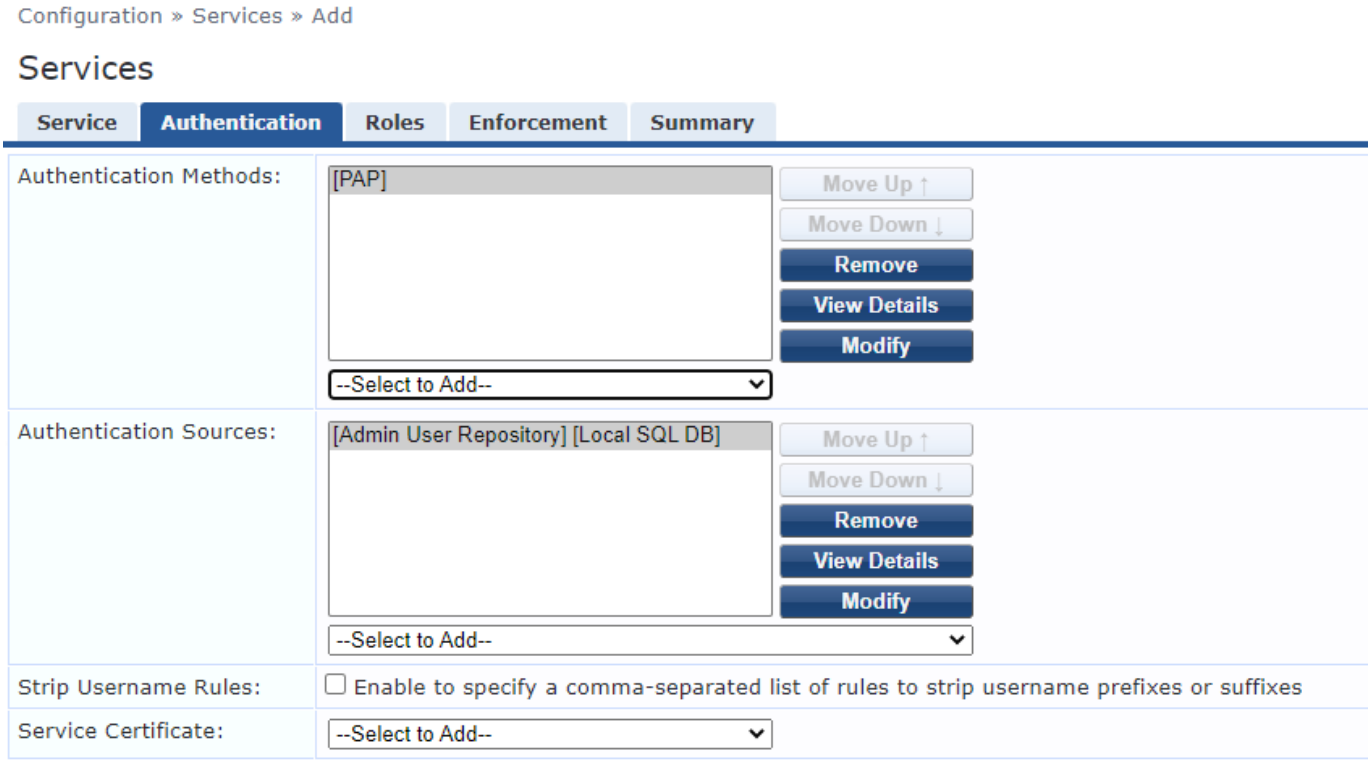
| Conditions | Actions |
|---|---|
| 1. (Tips:Role *EQUALS* PSM Admin) | PSM Admin User |

## Create PSM Authentication Service

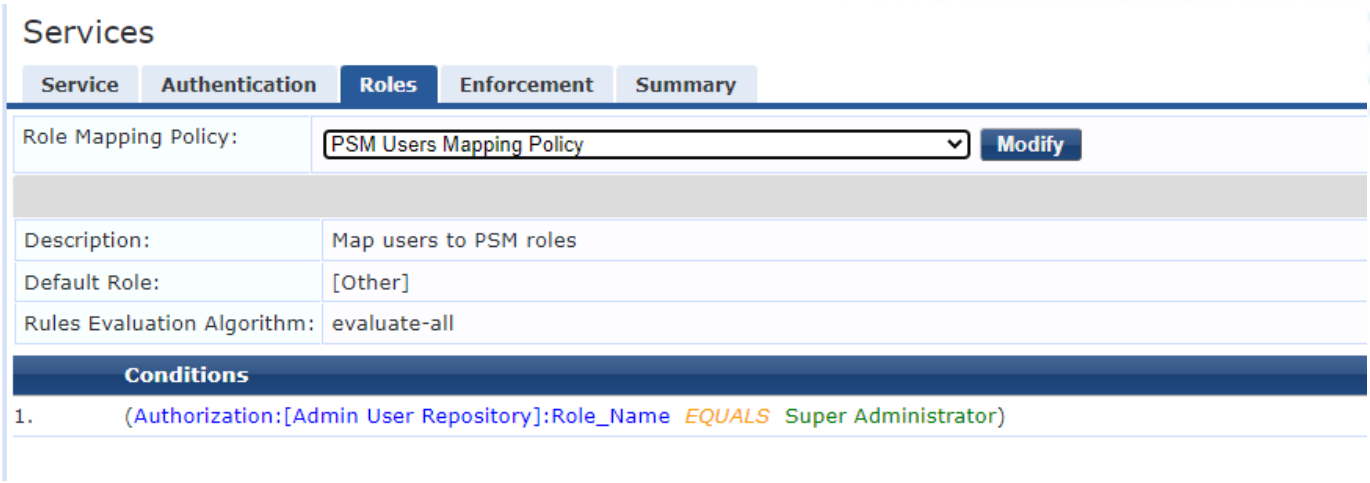
Create a new Service under **Configuration > Services**. In dropdown menu select **RADIUS Enforcement (Generic)**. In the Service Rule select **ALL of the following conditions**. Add Service rules **Connection > NAD-IP-Address > BELONGS_TO_GROUP > PSM** (group you created for PSM servers), and **Radius:IETF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



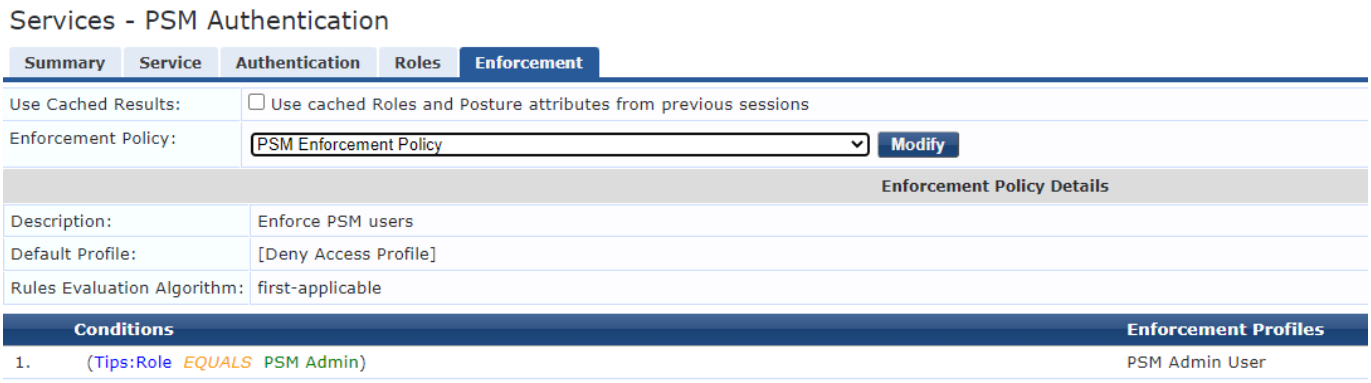

Click **Next**. Select Authentication Methods **[PAP]** and Authorization Source **[Admin User Repository]**. Click **Next**.



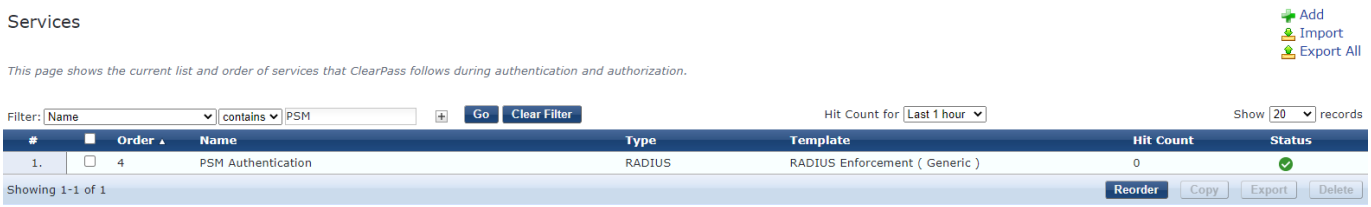

Select Role Mapping Policy (**PSM User Mapping Policy**) created in previous steps. Click **Next**.

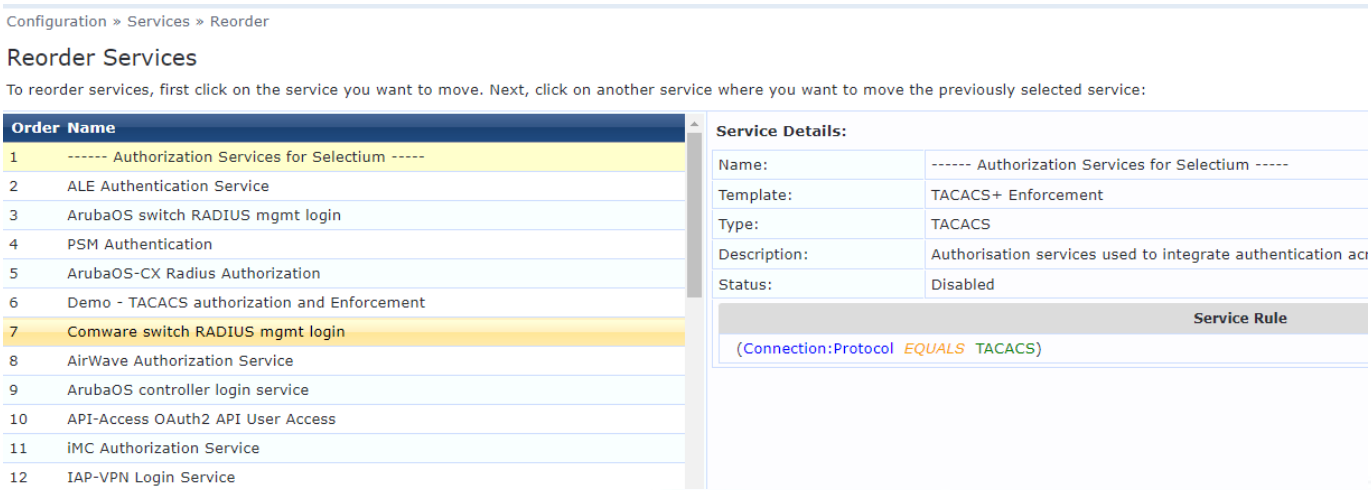



Select Enforcement Policy (**PSM Enforcement Policy**) created in previous steps. Click **Save** to save the Service.




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



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:**

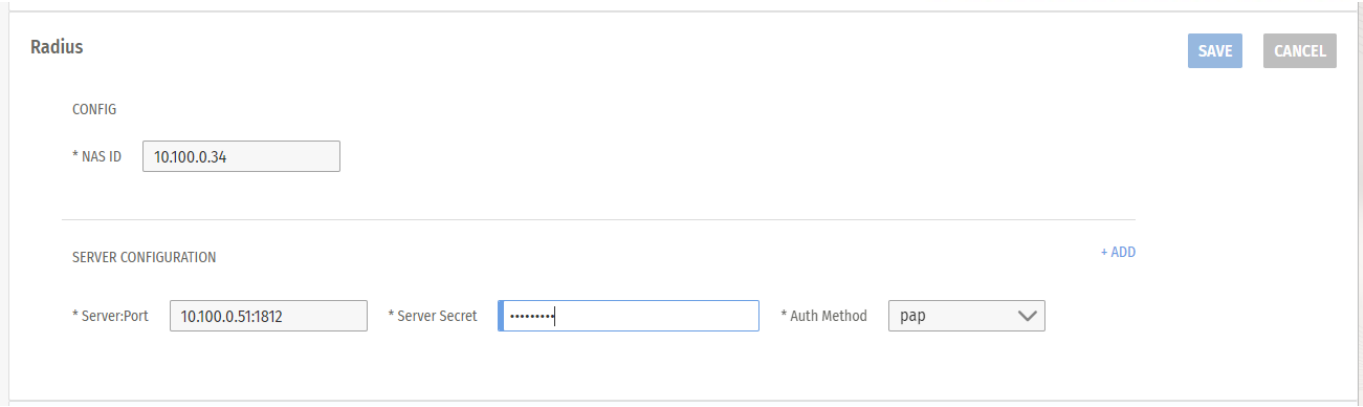
| | |
|---|---|
| Use Cached Results: | Disabled |
| Enforcement Policy: | PSM Enforcement Policy |

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**.

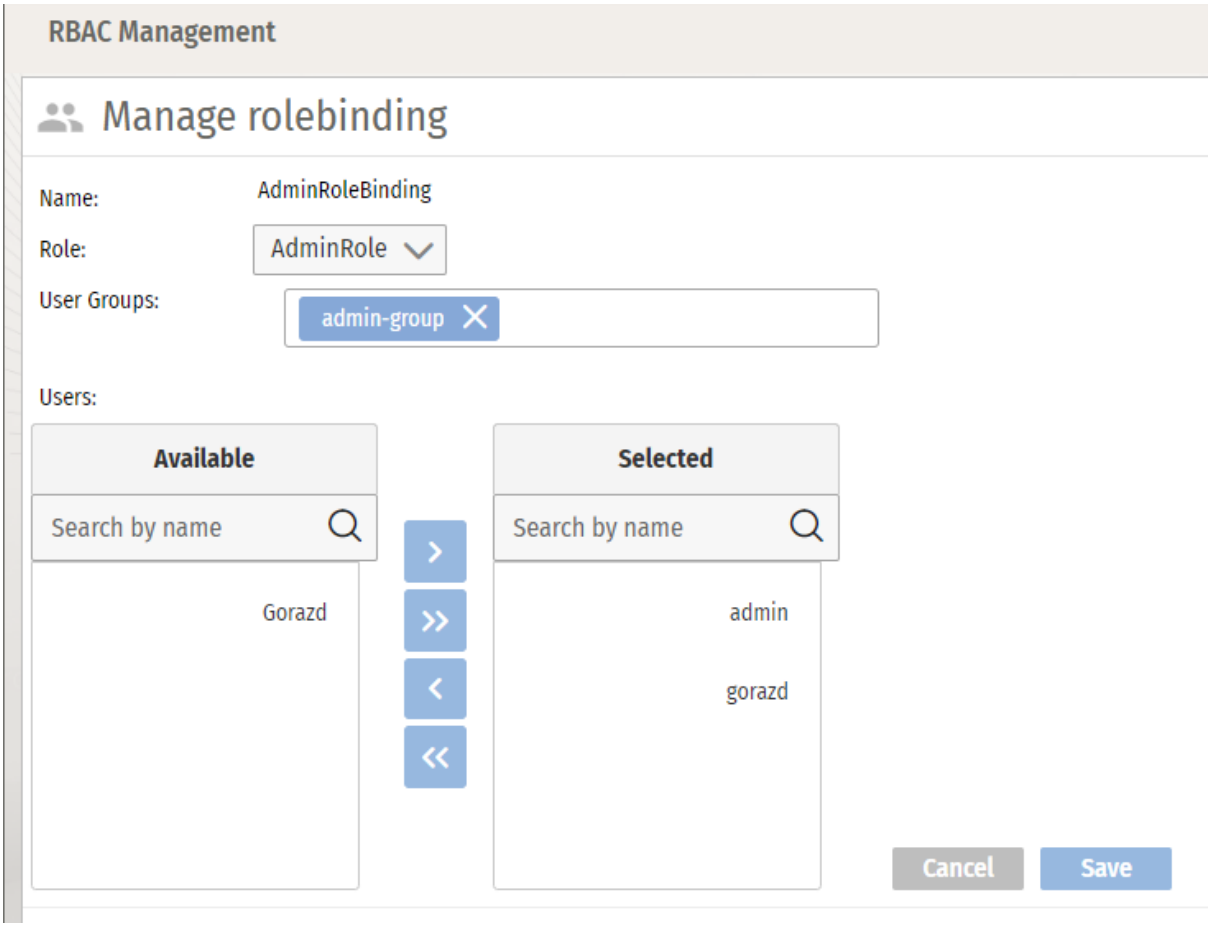



**NAS ID**: IP address of the PSM server/cluster[1]

**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.



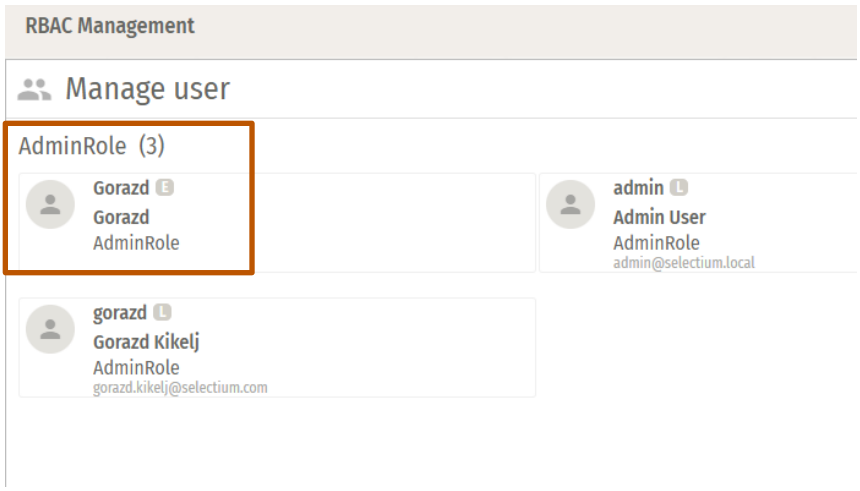

[1] Check chapter USING PSM NAS-ID WITH CLEARPASS SERVICE DEFINITION for cluster deployments

# TEST THE AUTHENTICATION

## Login into PSM using the RADIUS user

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

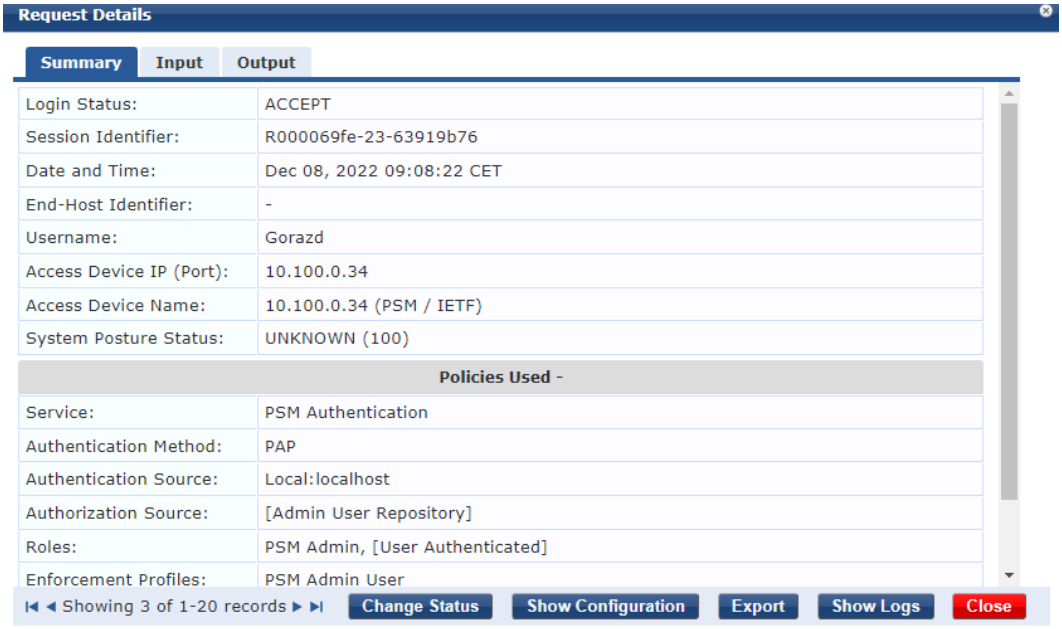

Once successfully logged in, you will notice that dynamic user is being created on PSM with the correct role.




## ClearPass Access Tracker Check

Check ClearPass Access tracker to see the authentication event.

| | | | | | |
|---|---|---|---|---|---|
| 3. | cppm-selectium | RADIUS | Gorazd | PSM Authentication | ACCEPT |

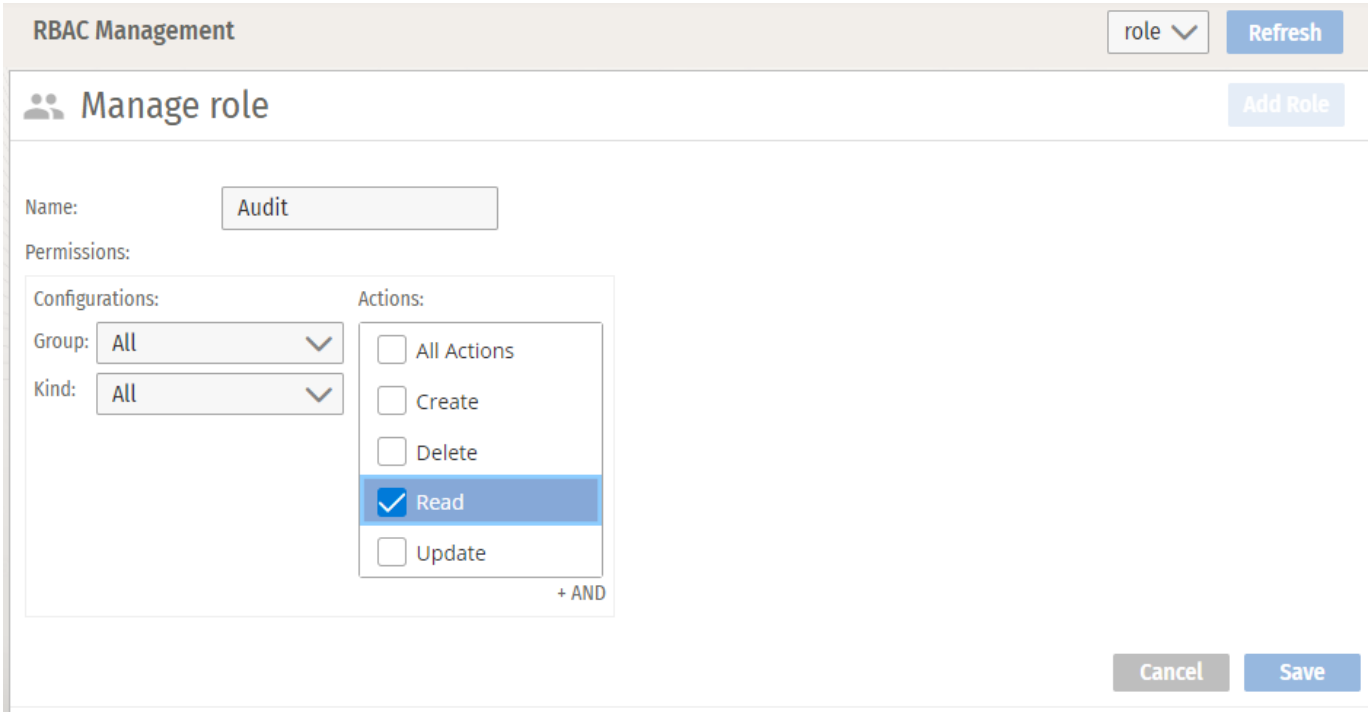



Expand RADIUS Response in Output tab to see returned attributes.

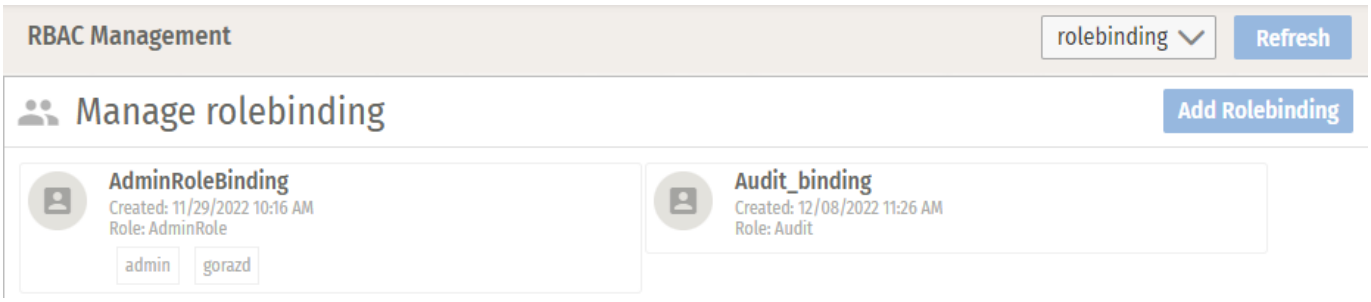
# NEW USER ROLE

## Create a new user group in PSM

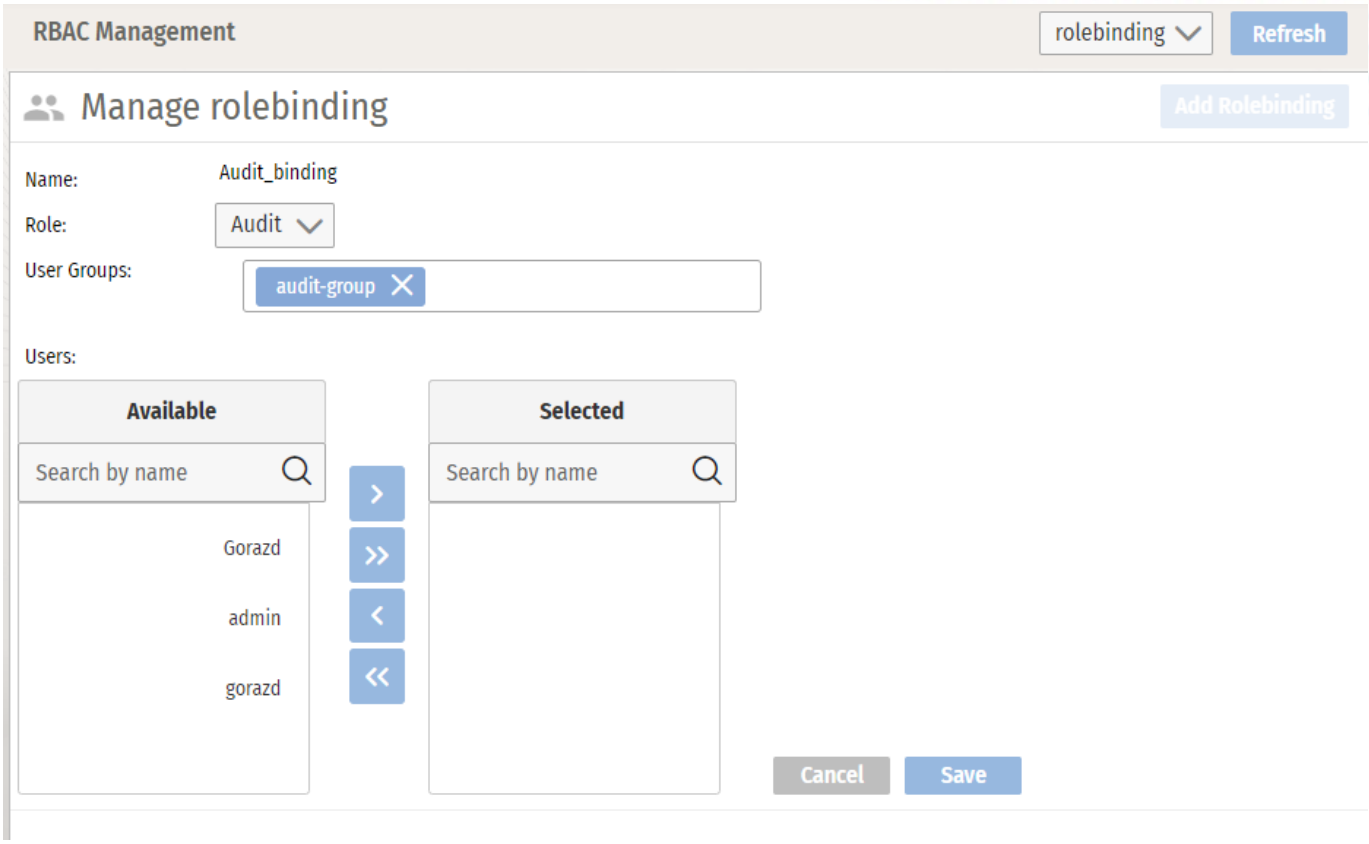
For new user group in PSM you need to create another role. In PSM GUI navigate to **User Management**. Select **role** at the top right pull down menu and select **Add Role**. This example create a role that can only read all the objects. Click **Save**.




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.

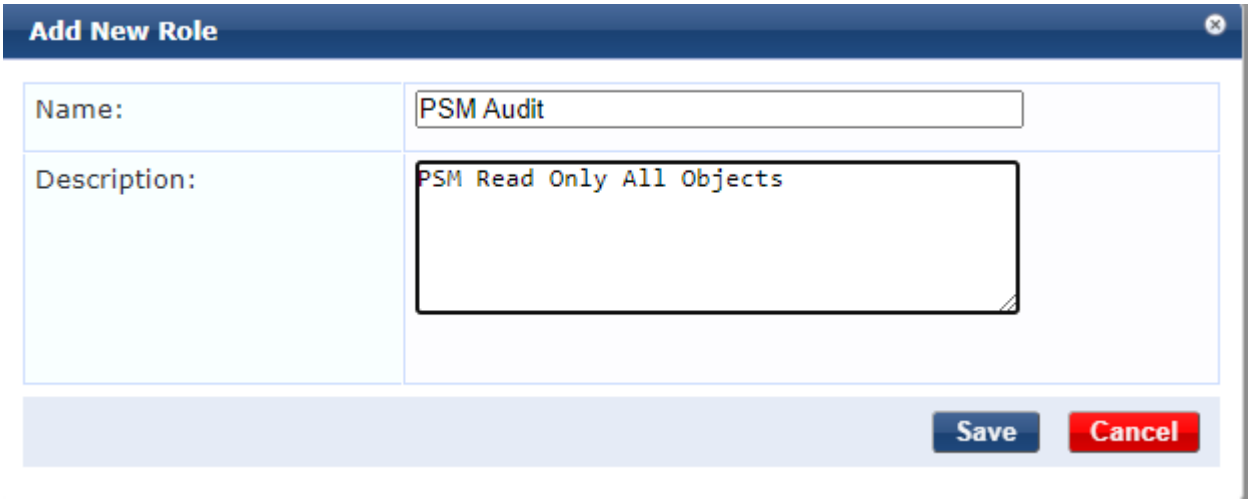



Click on the **Audit_binding** button and add a new User Group. In the example the group name is **audit-group**. Click **Save** to save the changes.

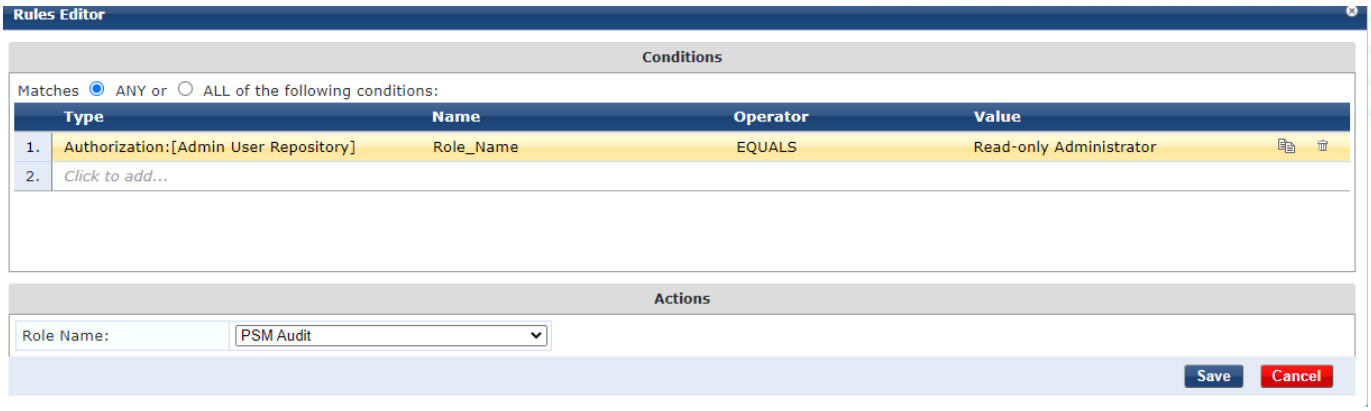



## Update Role Mapping Policy in ClearPass

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




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] |

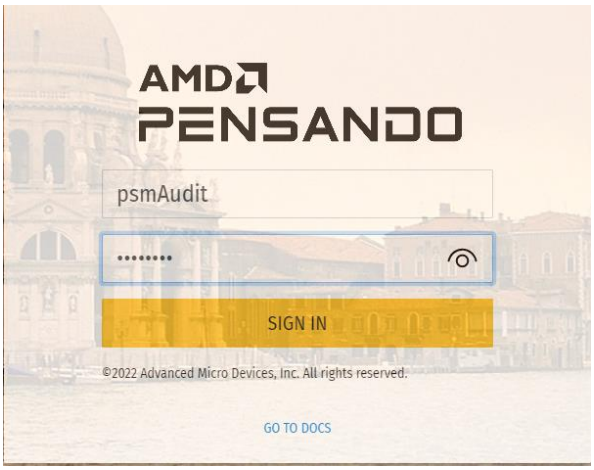
**Rules:**

| | |
|---|---|
| Rules Evaluation Algorithm: | First applicable |

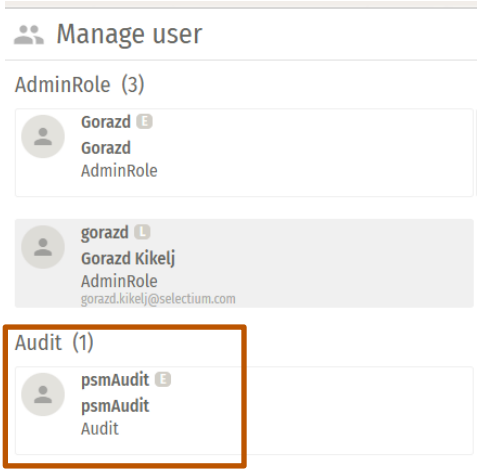
| | Conditions | Actions |
|---|---|---|
| 1. | (Tips:Role *EQUALS* PSM Admin) | PSM Admin User |
| 2. | (Tips:Role *EQUALS* PSM Audit) | PSM Audit User |

# Test the policy

Login as the read only user.



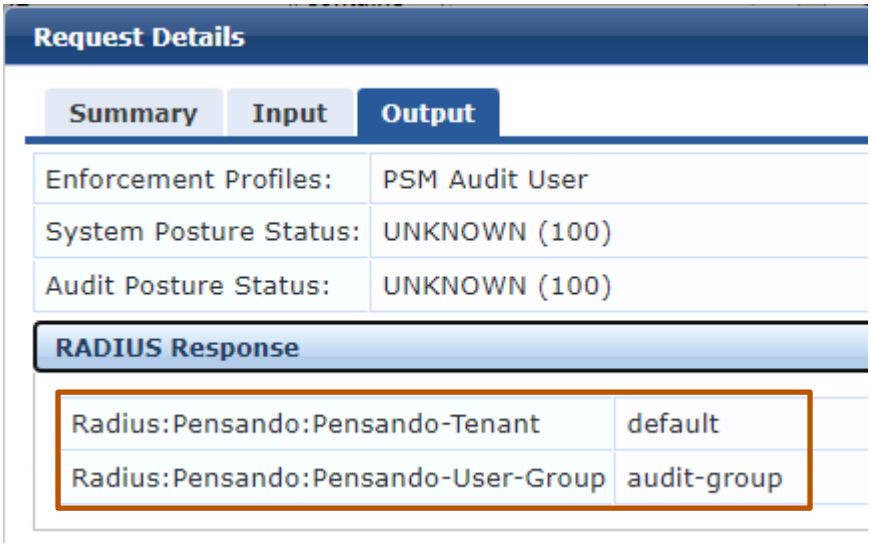

In User Management you will see a new dynamic user psmAudit.




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 |

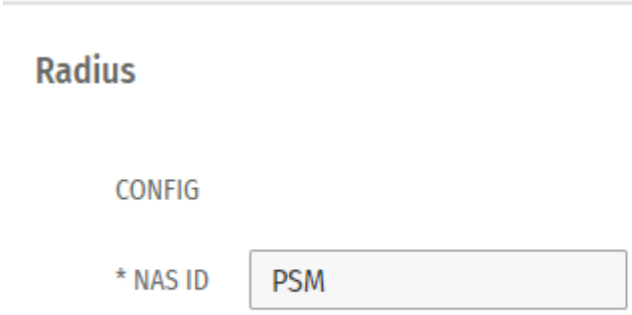
In Output tab you can check RADIUS attributes sent to PSM.



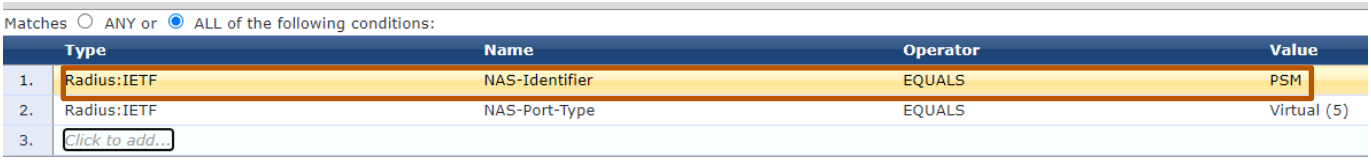
# USING PSM NAS-ID WITH CLEARPASS SERVICE DEFINITION

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.

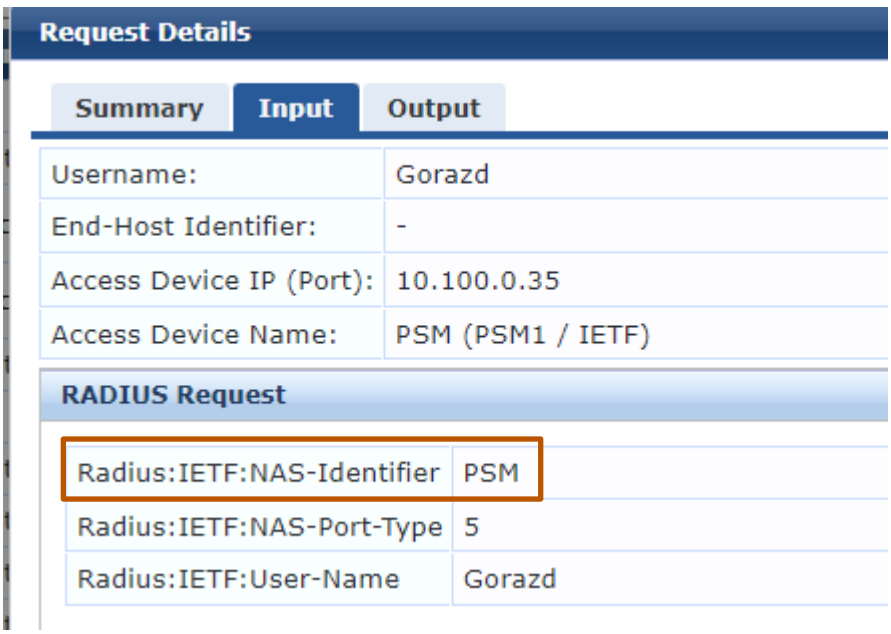
Go to **Auth Policy > Radius** and edit **NAS-ID** parameter. In the example configuration NAS-ID value is PSM.




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




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



# ADDITIONAL INFORMATION

Additional information is available on asp.arubanetworks.com.