



PACKETSHAPER ADMIN ACCESS USING 802.1x WITH CLEARPASS

In this article I'll try to explain how we can do radius authentication for administrator access in bluecoat packetshaper with Clearpass Policy manager.

BLUECOAT PACKETSHAPER WITH CLEARPASS

Here I assume that you have a packetshaper up & running. First thing you should know to perform this operation is packetshaper's administrative mode.

In packetshaper there are two mode

1. Touch [For read & write]
2. Look [For read only]

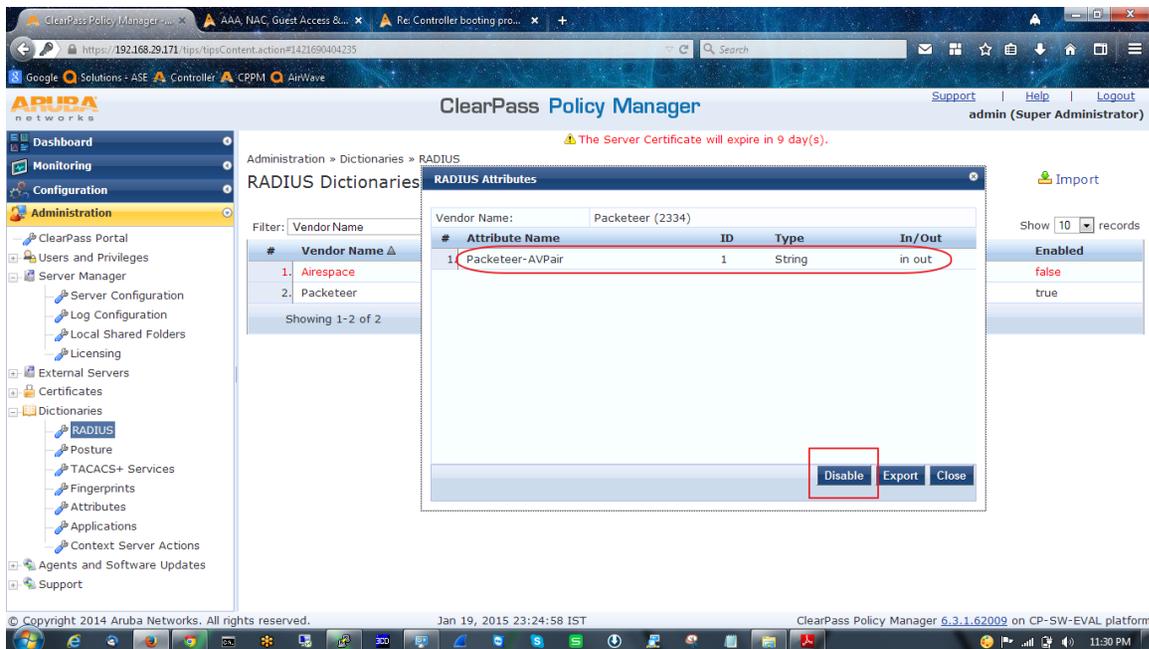
For details <https://bto.bluecoat.com/webguides/packetguide/11.1/nav/tasks/configure/setup-security.htm>

So here we'll do touch login. For that we need some special attribute called "access=touch". It should come from CPPM, through this attribute only packetshaper can understand 'oh! This is my administrator, so give him read & write access.

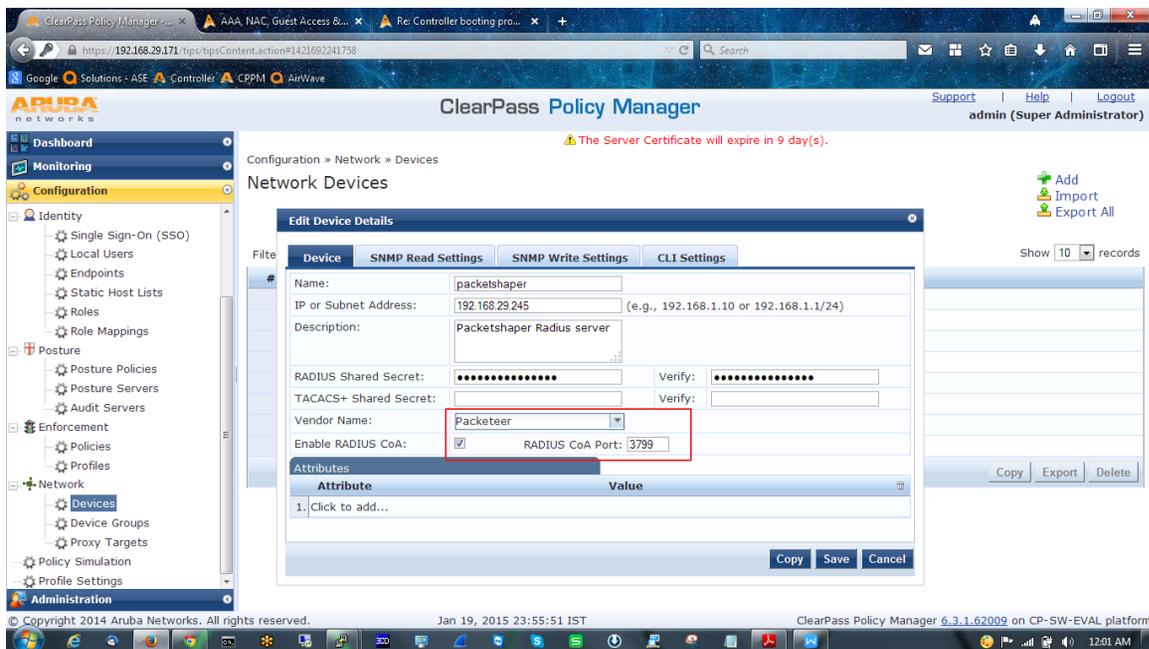
1. Configuring CPMM

- Log in to the CPPM & go to Administration » Dictionaries » RADIUS.

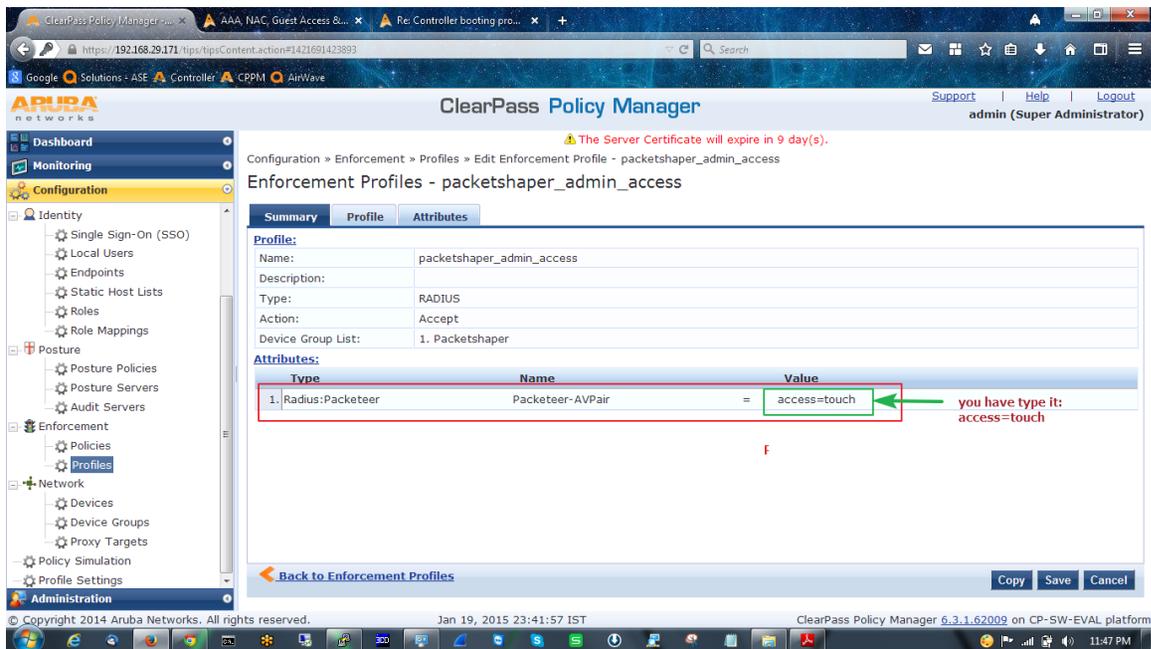
There you will get all predefined Vendor and VSA, [If you want you can import your own also] now go to Packeteer Vendor name and enable [by default it's disabled].



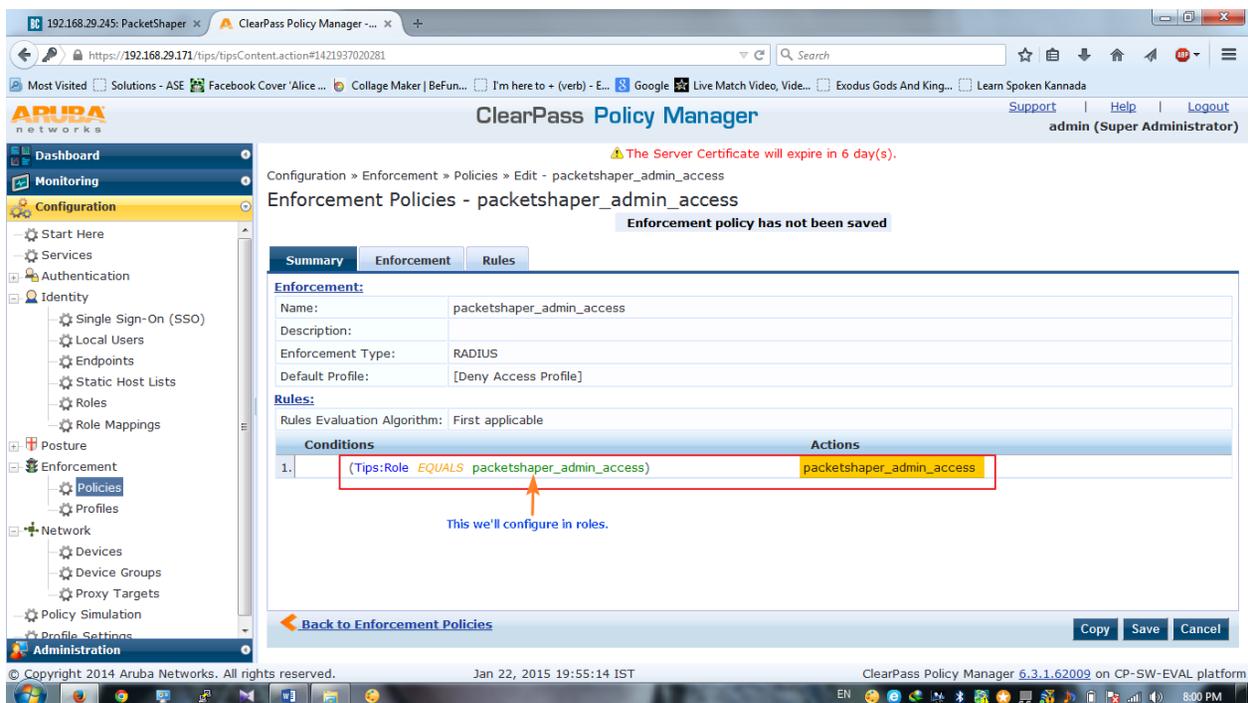
- Open Configuration » Network » Devices
- And add that Packetshaper, remember here you have to give vendor name [Packetshaper]
If you want you can create a Device group for this PS [Best Practice].



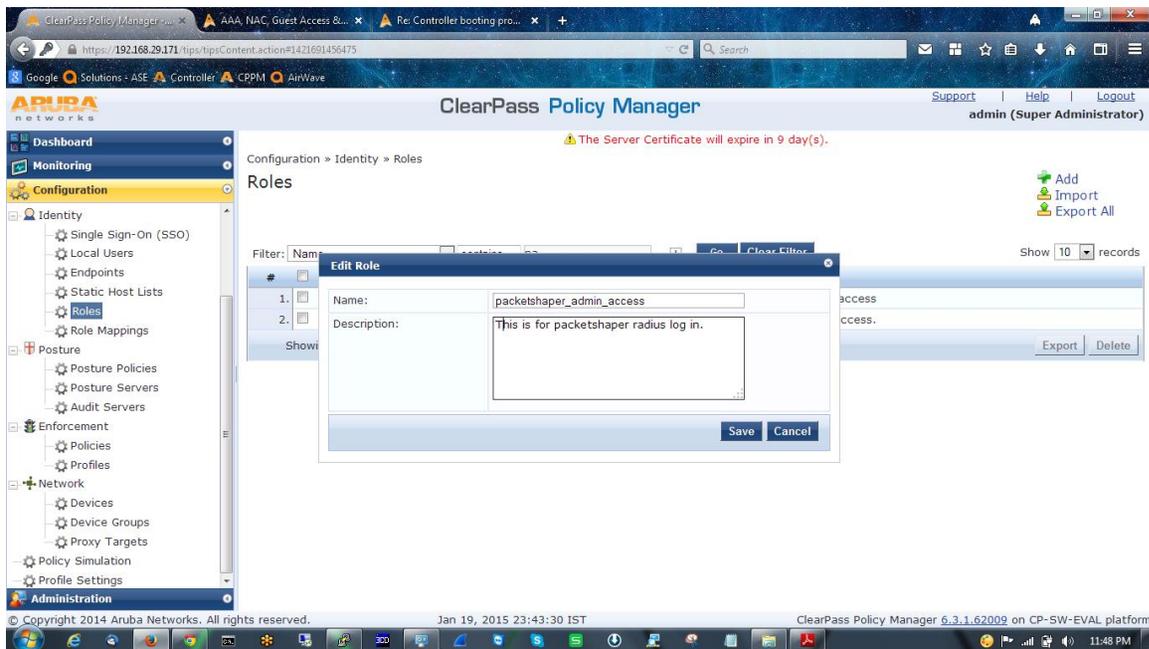
- Go to Configuration » Enforcement » Profiles »
- Add a Enforcement profile, & in attribute tab choose 'Radius: Packeteer' & value 'access=touch'
[you have to enter this manually, remember this is case sensitive]



- Switch to Configuration » Enforcement » Policies »
- Choose 'default role', create one Tips role with a value [enter manually & remember, because we have to create same 'Roles' for local user, this is case sensitive], assign the enforcement policy.

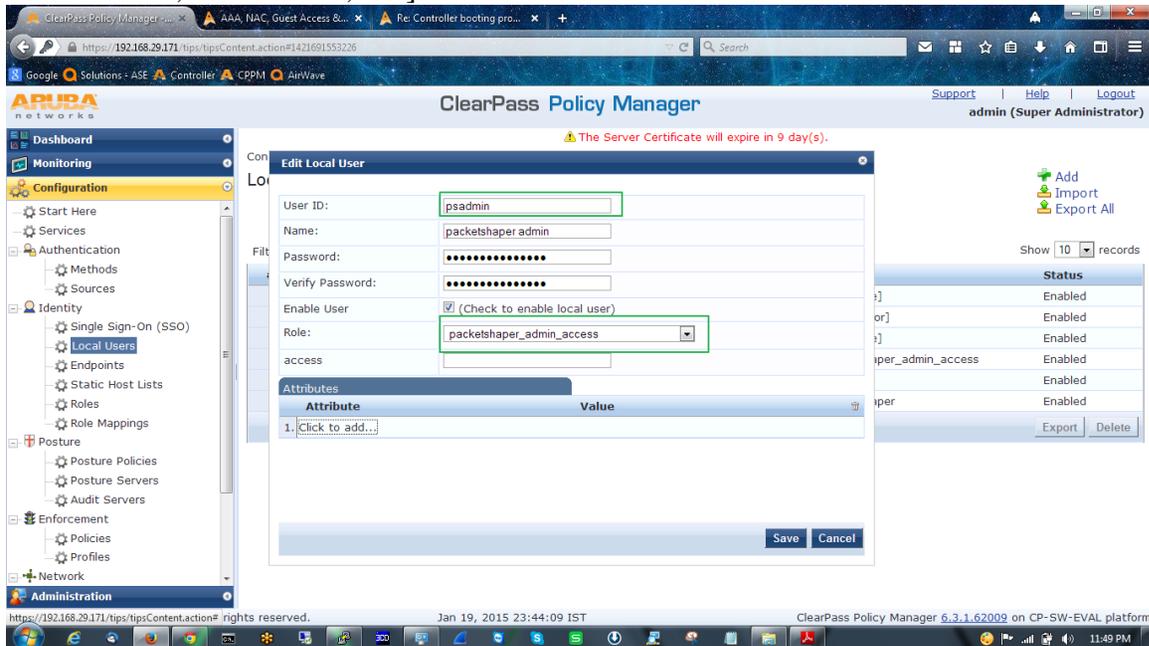


- Now open Configuration » Identity » Roles
- Assign the same name as assigned in enforcement policy. In my case both are < packetshaper_admin_access >



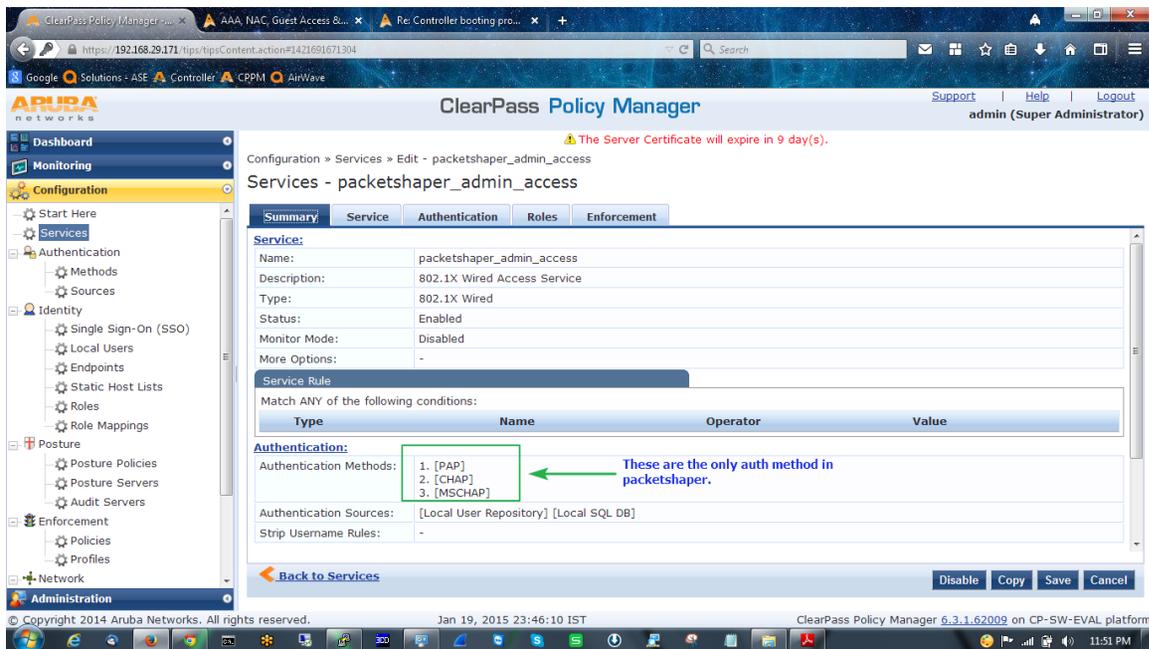
- Role mapping is not required, but you can configure if you want.
- Go to Configuration » Identity » Local Users

Create one user, and assigned that role, which we configured in Roles [This is the most important steps, because from here CPPM will start to retrieve the vendor specific attribute and vendor id. [Retrieving will be like this # user>Roles>Enforcement policy> Enforcement Profile> access=touch, & vendor id, etc.]

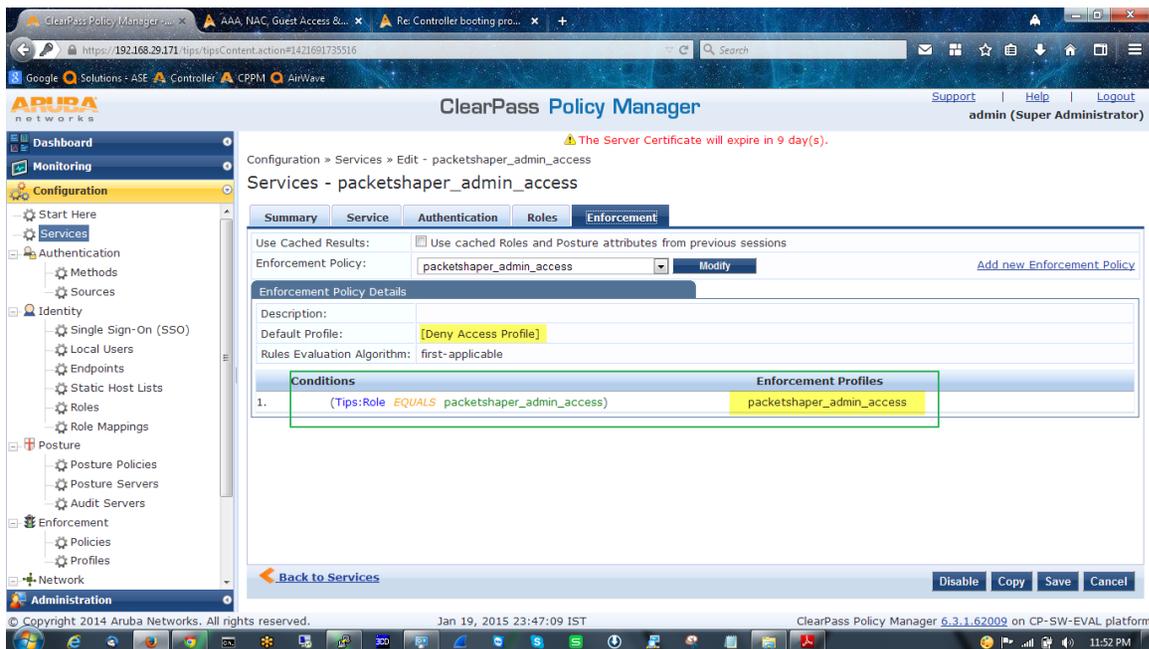


- Create one service [Configuration » Services],

Here I'll use Internal DB as an authentication source, if you want you can use AD for authentication source.



In Enforcement add the appropriate enforcement profile.



2. Configuring Packetshaper :

- Login to the PS as touch [read & write], & go to setup>Radius client

In the authentication host tab, put the IP address of the CPPM, turn on the authentication. That's all.

Unit: 117-10017460 Traffic Discovery: Off

Choose Setup Page: [RADIUS client]

RADIUS Client settings

apply changes reset form

RADIUS Authentication will be used if **Authentication** is turned on *and* an **Authentication Host** is entered.
 RADIUS Accounting will be used if **Accounting** is turned on *and* an **Accounting Host** is entered.

Authentication: on here you can select, which method packetshaper will use for auth

Authentication method: MSCHAP

Primary Authentication Host: 192.168.29.171 **Port:** 1812 **Shared Secret:** [REDACTED]

Secondary Authentication Host: [REDACTED] **Port:** [REDACTED] **Shared Secret:** [REDACTED]

default: 1812

Accounting: off

Primary Accounting Host: 192.168.29.171 **Port:** 1813 **Shared Secret:** [REDACTED]

Secondary Accounting Host: [REDACTED] **Port:** [REDACTED] **Shared Secret:** [REDACTED]

default: 1813

Retry limit: 3

Retry interval (seconds): 5

ALL HAS DONE, IT'S TIME TO CHECK OUTPUT

✓ In CPPM Access Tracker.

ClearPass Policy Manager

admin (Super Administrator)

Request Details

Summary Input Output

Session Identifier: R0000025e-01-54b4a66

Date and Time: Jan 19, 2015 23:48:14 IST

End-Host Identifier: -

Username: psadmin

Access Device IP/Port: 192.168.29.245

System Posture Status: UNKNOWN (100)

Policies Used -

Service:	packetshaper_admin_access
Authentication Method:	MSCHAP
Authentication Source:	Local:localhost
Authorization Source:	[Local User Repository]
Roles:	[User Authenticated], packetshaper_admin_access
Enforcement Profiles:	packetshaper_admin_access
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-50 records

Change Status Export Show Logs Close

Request ID	Request Timestamp	Status
14	2015/01/19 23:48:14	ACCEPT
	2015/01/19 23:46:55	
	2015/01/19 23:41:15	
	2015/01/19 23:40:50	
	2015/01/19 23:39:55	
	2015/01/19 23:38:08	
	2015/01/19 23:37:58	
	2015/01/19 23:36:39	
	2015/01/19 23:35:42	
	2015/01/19 23:23:04	
	2015/01/19 23:22:42	
	2015/01/19 23:21:28	
	2015/01/19 23:21:12	
	2015/01/19 23:20:07	

The screenshot shows the ClearPass Policy Manager interface. The 'Request Details' window is open, displaying a rejected RADIUS request. The 'Summary' tab is selected, showing the following details:

Field	Value
Authentication:Full-Username	psadmin
Authentication:Full-Username-Normalized	psadmin
Authentication:MacAuth	NotApplicable
Authentication:OuterMethod	MSCHAP
Authentication:Posture	Unknown
Authentication:Source	[Local User Repository]
Authentication:Status	User
Authentication:Username	psadmin
Authorization:Sources	[Local User Repository]
Connection:Dest-IP-Address	192.168.29.171
Connection:Dest-Port	1812
Connection:NAD-IP-Address	192.168.29.245
Connection:Protocol	RADIUS
Connection:Src-IP-Address	192.168.29.245
Connection:Src-Port	1028

The request status is 'REJECT'. The user is 'psadmin' and the source is 'packetsnaper_admin_a'. The timestamp is 2015/01/21 10:19:48.

The screenshot shows the ClearPass Policy Manager interface. The 'Request Details' window is open, displaying an accepted RADIUS request. The 'Summary' tab is selected, showing the following details:

Field	Value
Enforcement Profiles	packetsnaper_admin_access
System Posture Status	UNKNOWN (100)
Audit Posture Status	UNKNOWN (100)

The 'RADIUS Response' section shows: Radius:Packeteer:Packeteer-AVPair access=touch. The request status is 'ACCEPT'. The user is 'suman' and the source is 'packetsnaper user'. The timestamp is 2015/01/19 23:20:07.

✓ In Clearpass policy simulation.

ClearPass Policy Manager

Configuration » Policy Simulation » Edit - packetshaper_admin_access_test

Policy Simulation - packetshaper_admin_access_test

Simulation Attributes Results

Name: packetshaper_admin_access_simulation

Description:

Type: Chained Simulation

Simulation Details

Test end-to-end policy evaluation that includes Role-Mapping and Enforcement Policies, given a Service and input details

Service: packetshaper_admin_access

Authentication Source: [Local User Repository]

Username: psadmin

Test Date and Time:

Back to Policy Simulation Copy Save Cancel

Copyright 2014 Aruba Networks. All rights reserved. Jan 22, 2015 09:18:30 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

ClearPass Policy Manager

Configuration » Policy Simulation » Edit - packetshaper_admin_access_simulation

Policy Simulation - packetshaper_admin_access_simulation

Simulation Attributes Results

Summary -

Status	Allow Access
Roles	[User Authenticated], packetshaper_admin_access
System Posture Status	UNKNOWN (100)
Enforcement Profiles	packetshaper_admin_access

Radius Output Attributes -

Radius:Packeteer:Packeteer-AVPair	access=touch
-----------------------------------	--------------

Back to Policy Simulation Copy Save Cancel

Copyright 2014 Aruba Networks. All rights reserved. Jan 22, 2015 09:18:36 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

✓ In Bluecoat Packetshaper.

```
192.168.29.245 - PuTTY
login as: psadmin
Login: psadmin
Password:
RADIUS login, psadmin granted touch access.
PacketShaper v8.3.491 2010-08-12
Copyright (c) 1996-2010, Blue Coat Systems, Inc. All rights reserved.
Packet shaping: off.
OUTSIDE interface down
PacketShaper# radius login psadmin
psadmin# RADIUS Authentication OK
Vendor-Specific: access=touch
PacketShaper# radius session
-----
ID          Status      Age      Idle      Limit    Type Access User Name
-----
54bd4c0b logged in   38 secs  0 secs   60 mins  CLI  touch psadmin
54bd4b70 logged in  190 secs 1 secs   60 mins  WUI  touch psadmin
54bd3ba7 logged in   70 mins 269 secs 60 mins  CLI  touch suman
54bd1c0b logged in  205 mins 204 mins 60 mins  WUI  touch suman
PacketShaper#
```

you can use this command for checking radius is working or not
PS# radius login <user> <password>

THANK YOU