



**PACKETSHAPER ADMIN ACCESS USING RADIUS WITH CLEARPASS**

In this article I’ll try to explain how we can do radius authentication for administrator access in bluecoat packetshaper with Clearpasss 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]

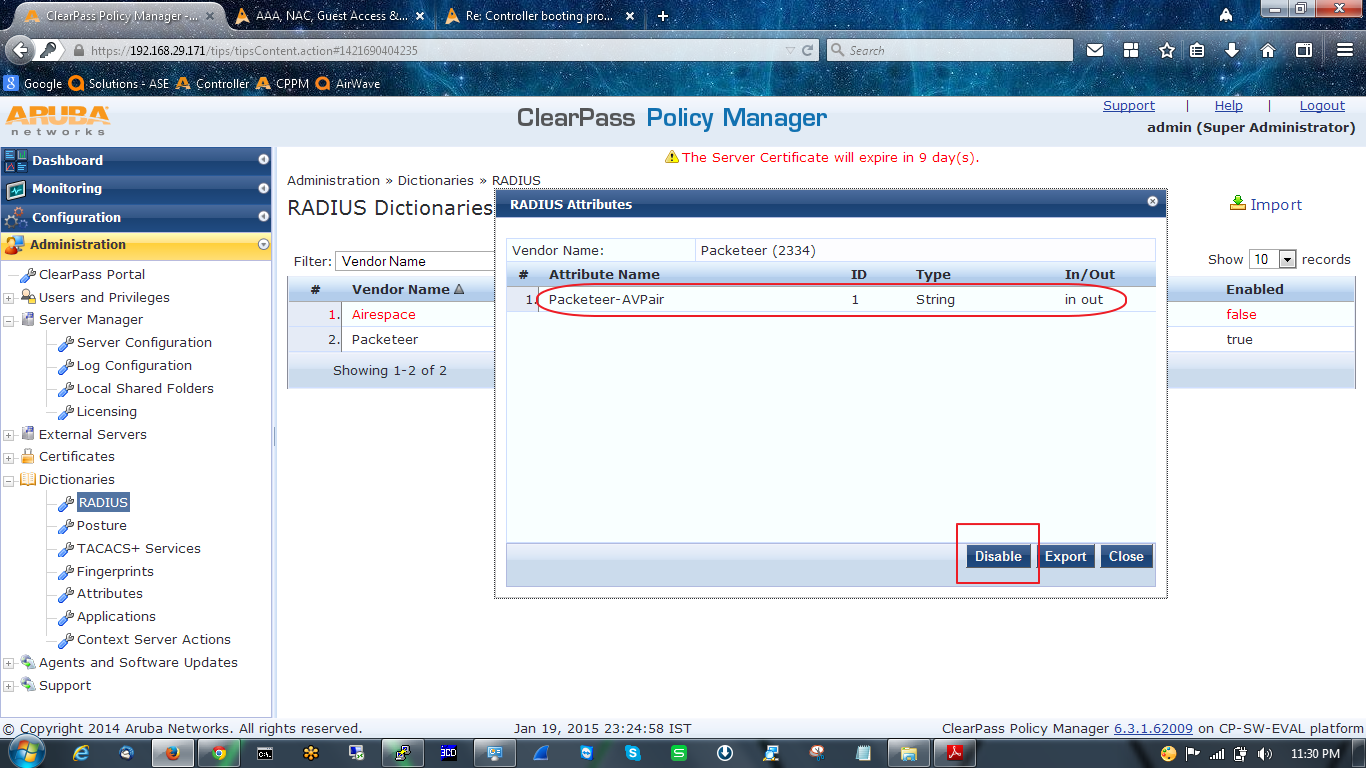
# For details <https://bto.bluecoat.com/webguides/packetguide/11.1/nav/tasks/configure/setup-security.htm>

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.

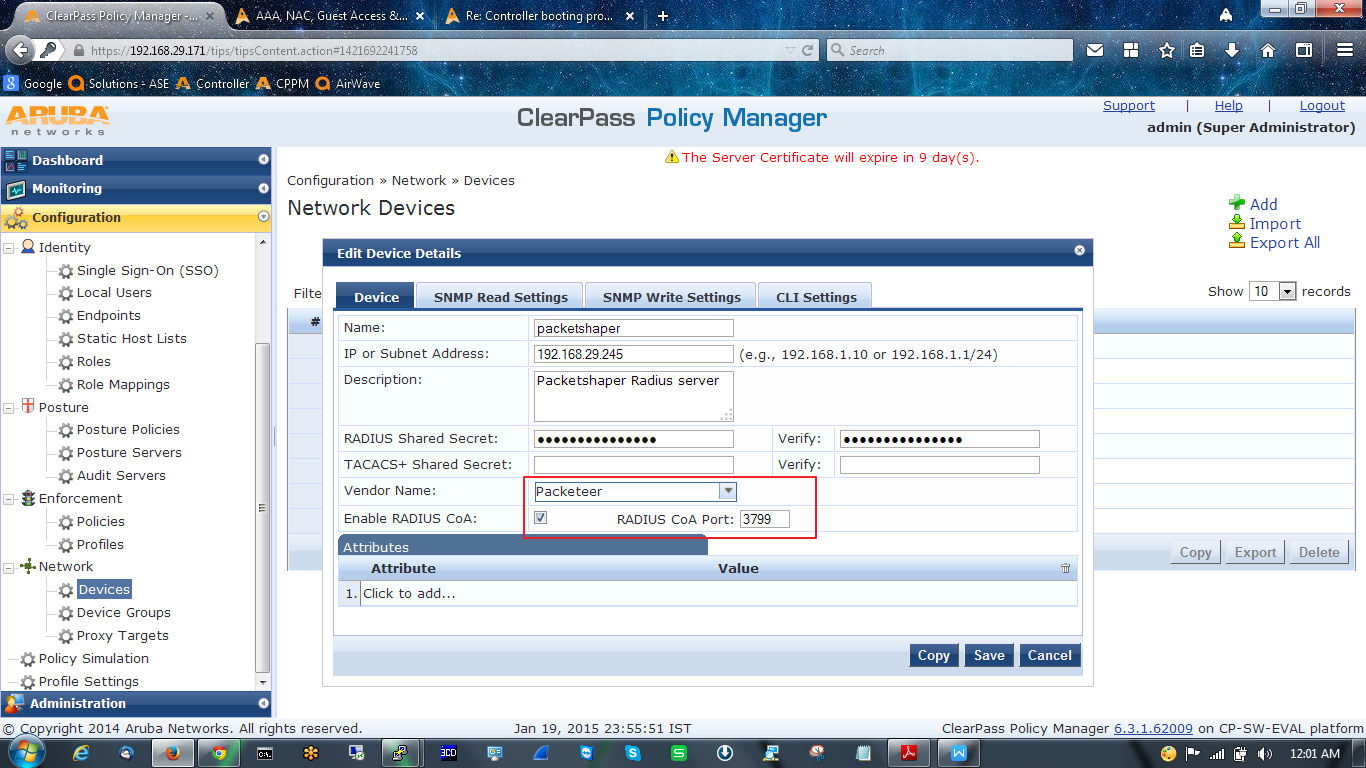
There you will get all predefined Vendor and VSA, [If you want you can import your own also] now go to Packeteer Vendor name and enable [by default it’s disabled].



* Open Configuration » Network » Devices

And add that Packetshaper, remember here you have to give vendor name [Packetshaper]

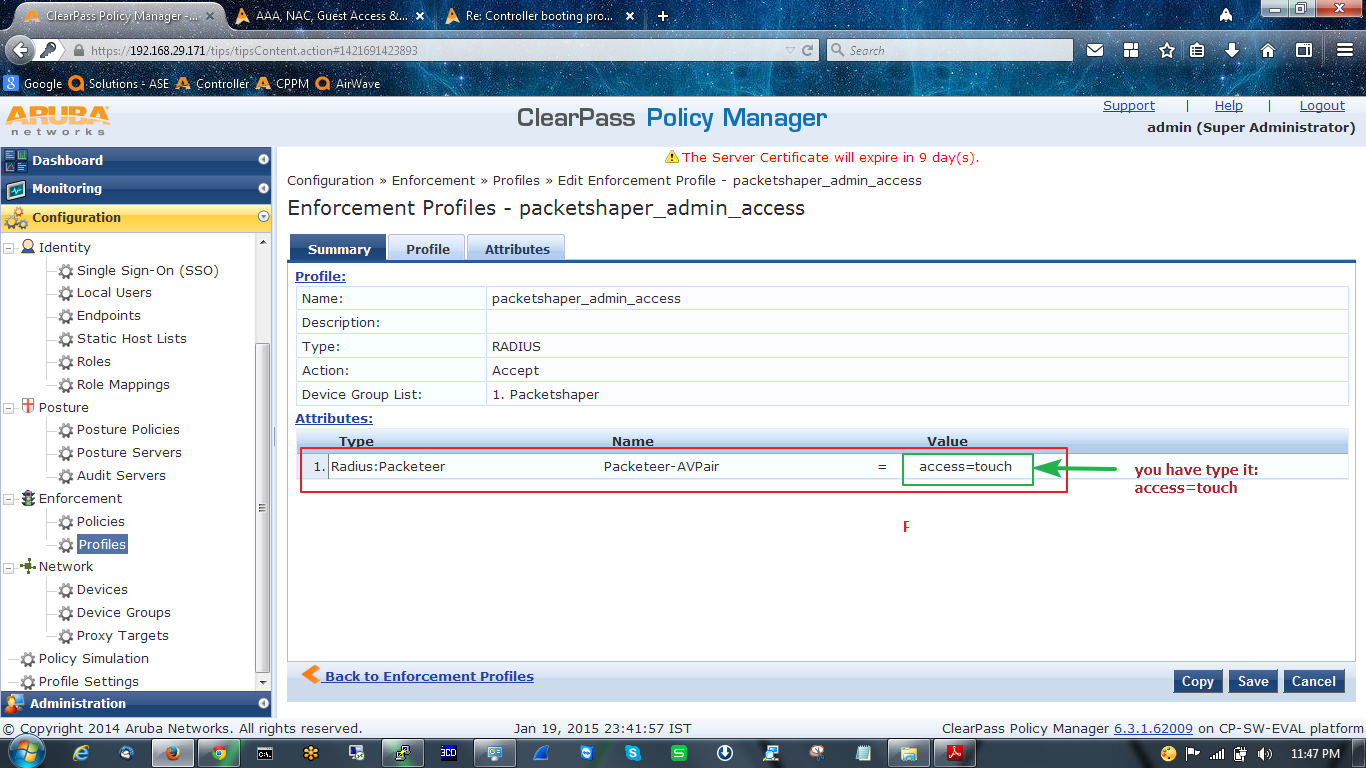
If you want you can create a Device group for this PS [Best Practice].



* Go to Configuration » Enforcement » Profiles »

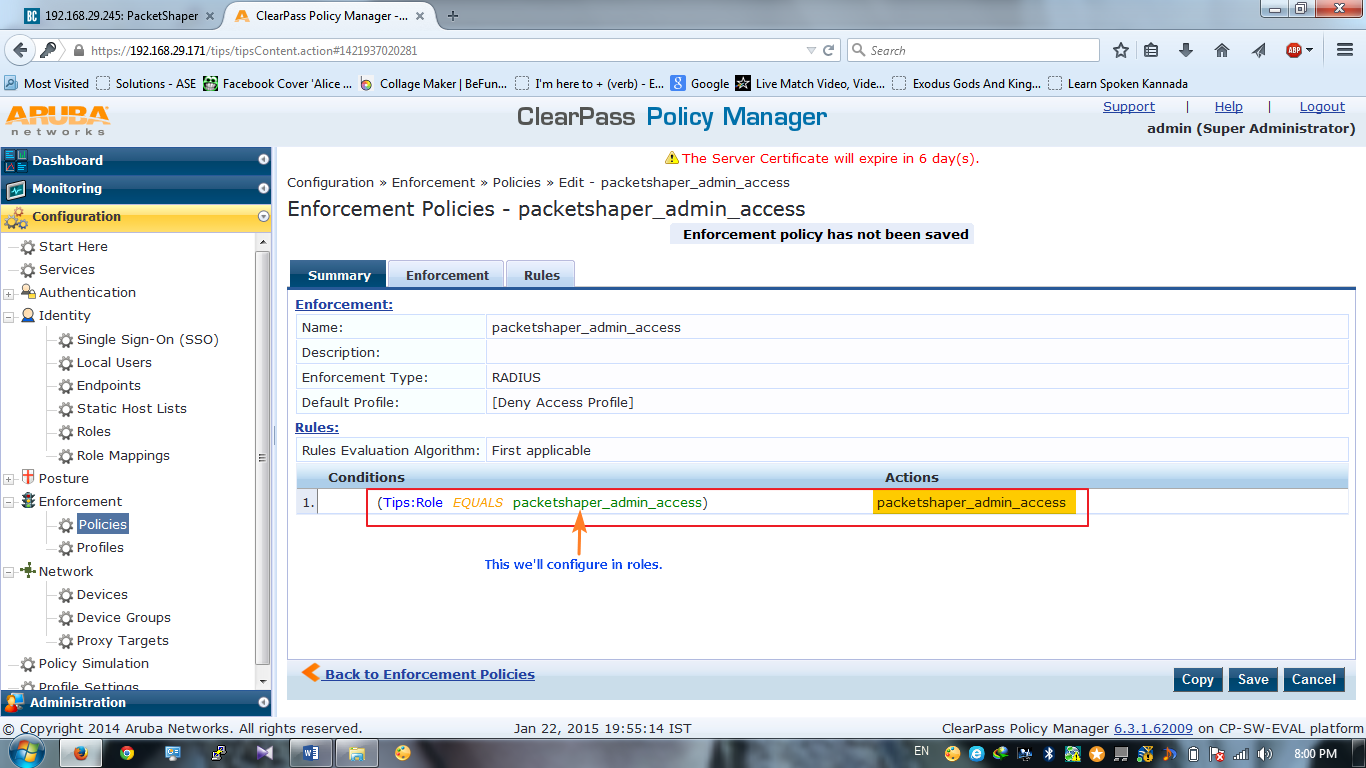
Add a Enforcement profile, & in attribute tab choose ‘Radius: Packeteer’ & value ‘access=touch’

[you have to enter this manually, remember this is case sensitive]



* Switch to Configuration » Enforcement » Policies »

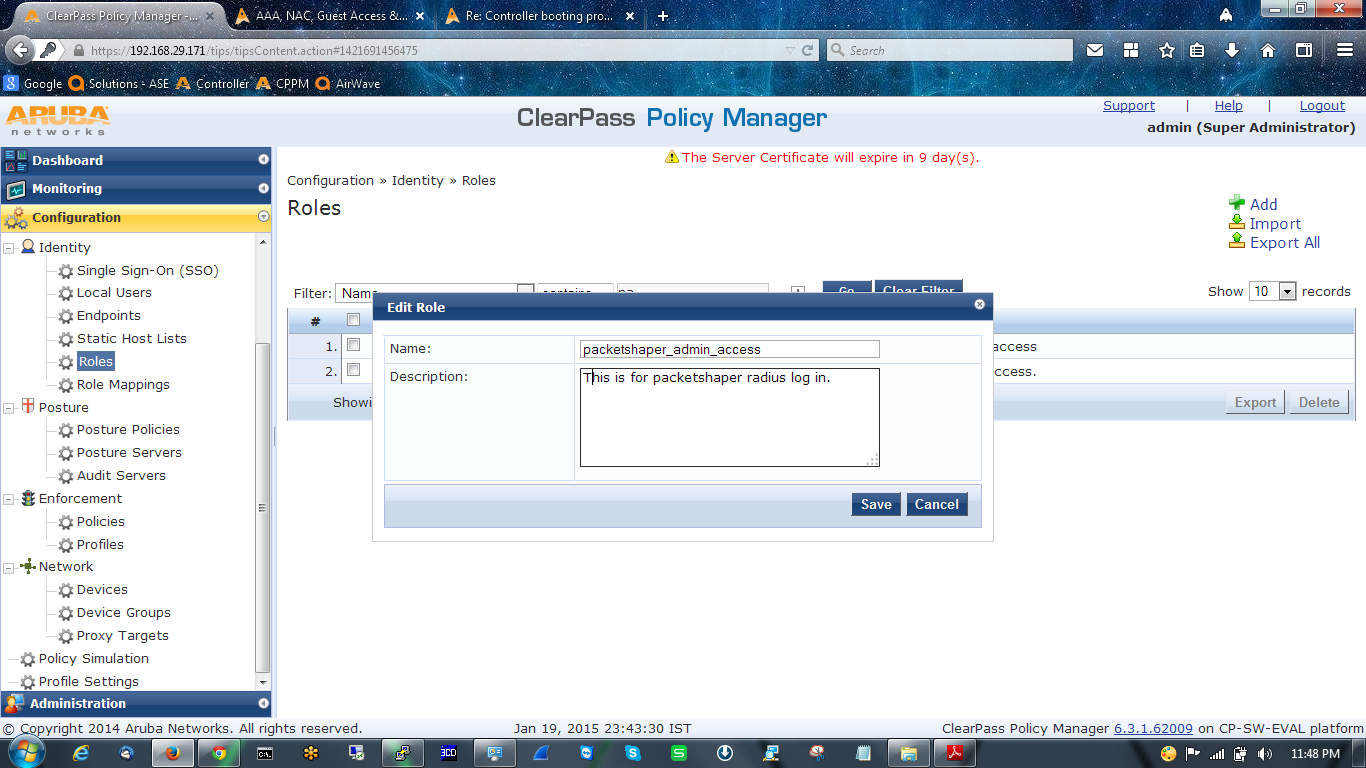
Choose ‘default role’, create one Tips role with a value [enter manually & remember, because we have to create same ‘Roles’ for local user, this is case sensitive], assign the enforcement policy.



* Now open Configuration » Identity » Roles

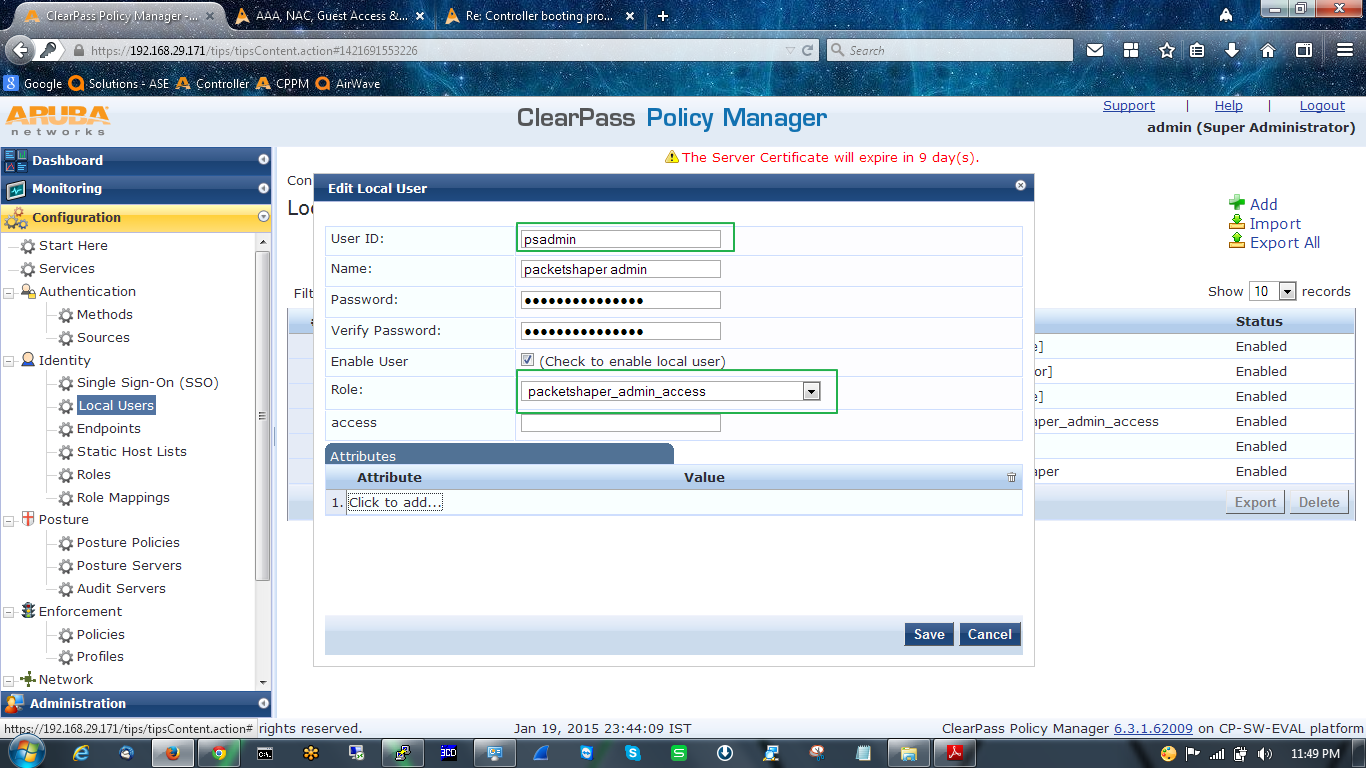
Assign the same name as assigned in enforcement policy. In my case both are

< 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.]

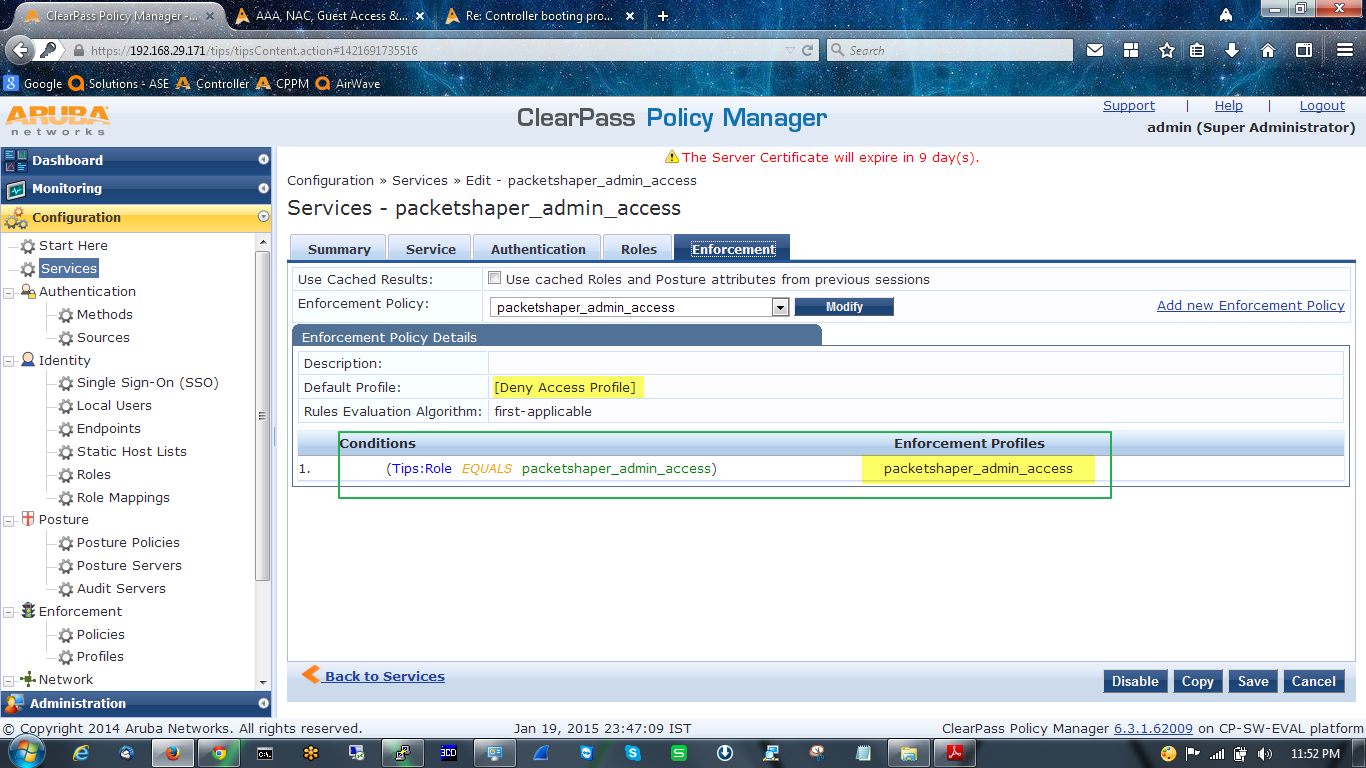


* Create one service [Configuration »Services],

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



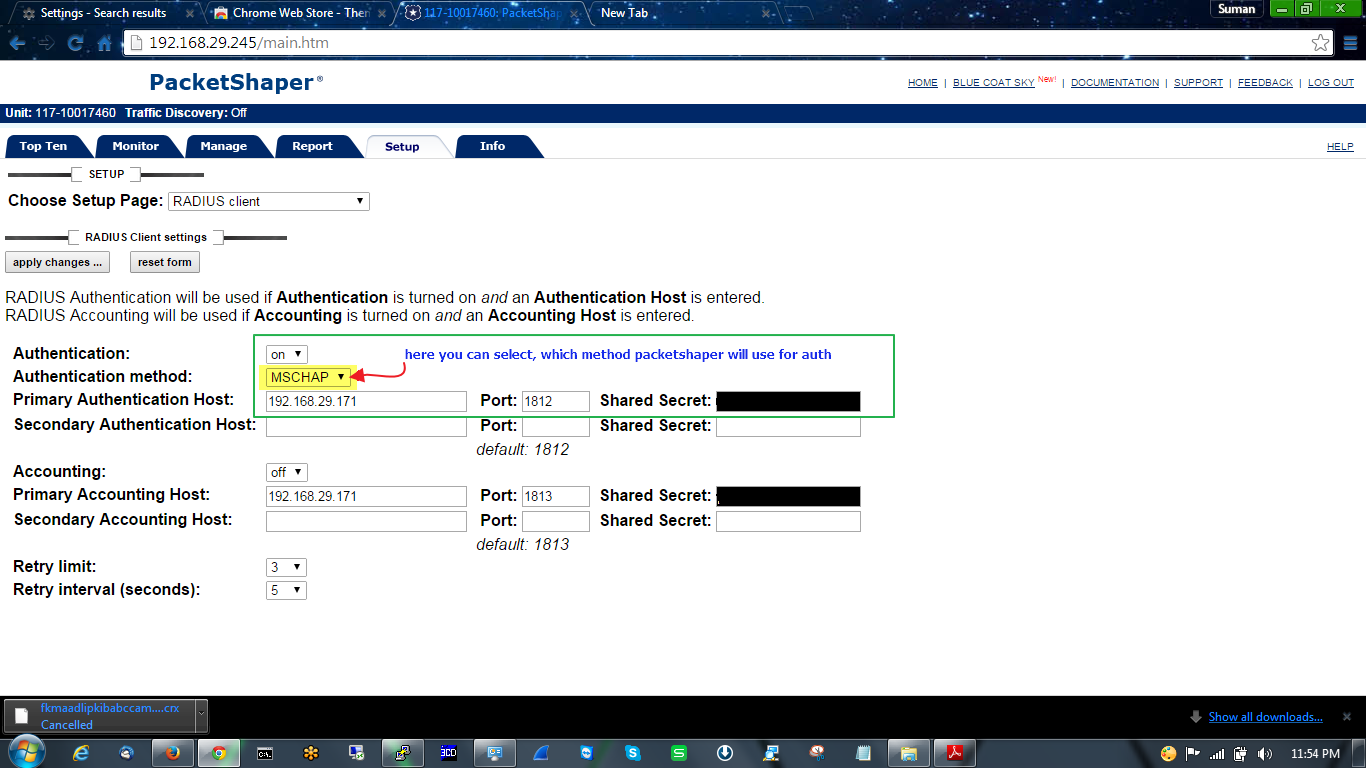
In Enforcement add the appropriate enforcement profile.



1. **Configuring Packetshaper :**

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

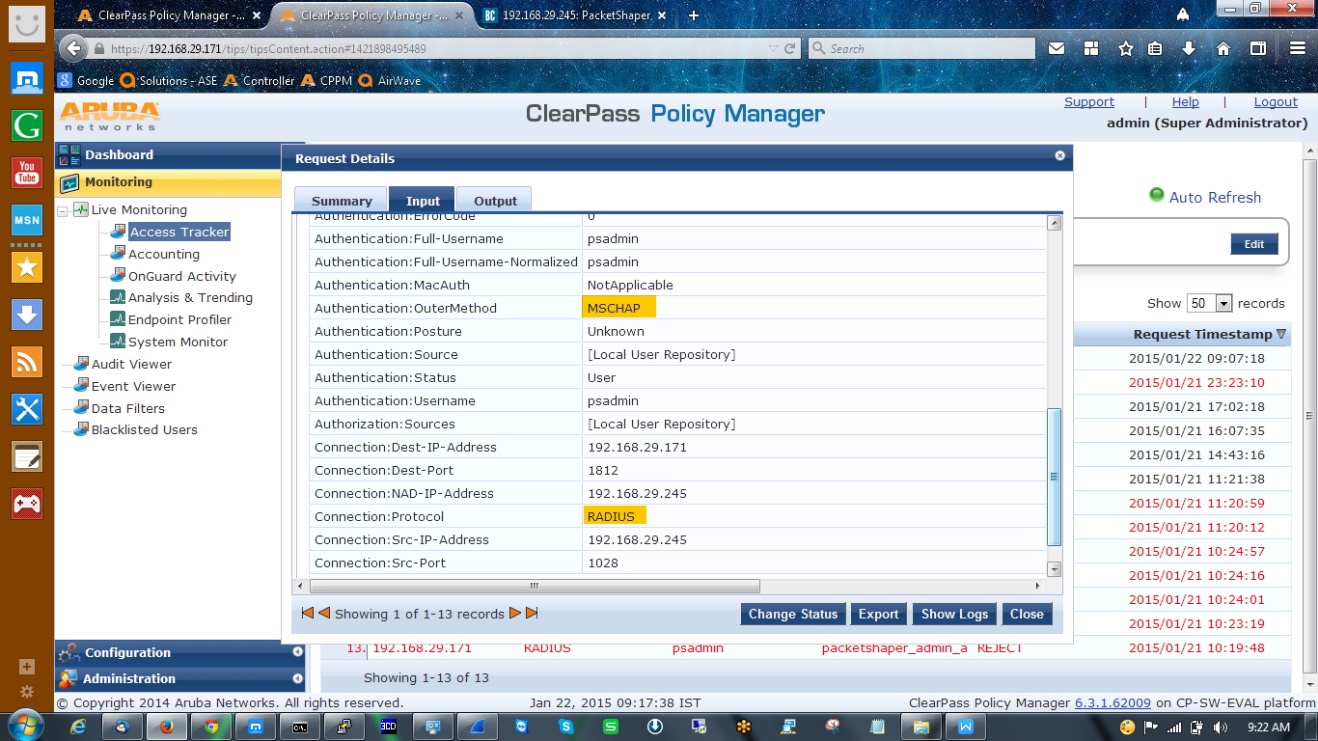
In the authentication host tab, put the IP address of the CPPM, turn on the authentication. That’s all.



**ALL HAS DONE, IT’S TIME TO CHECK OUTPUT**

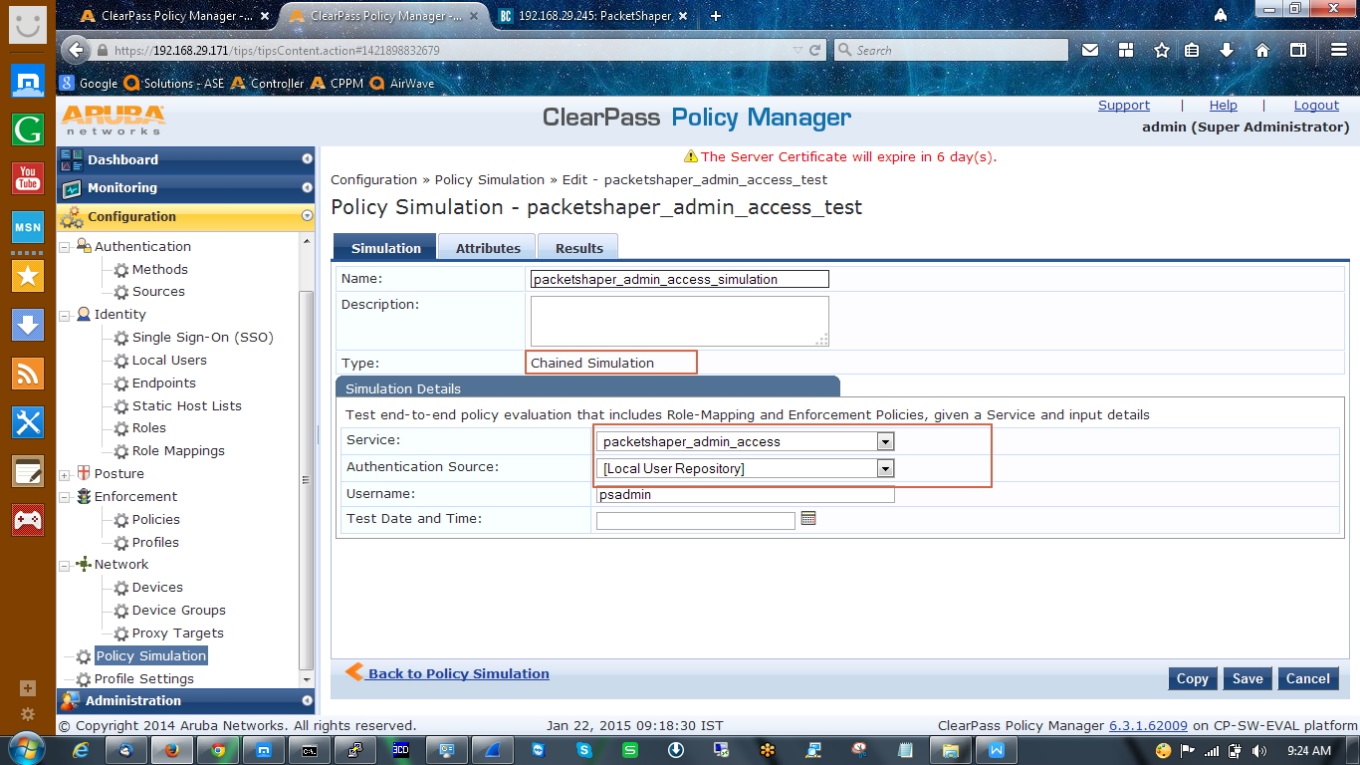
* **In CPPM Access Tracker.**

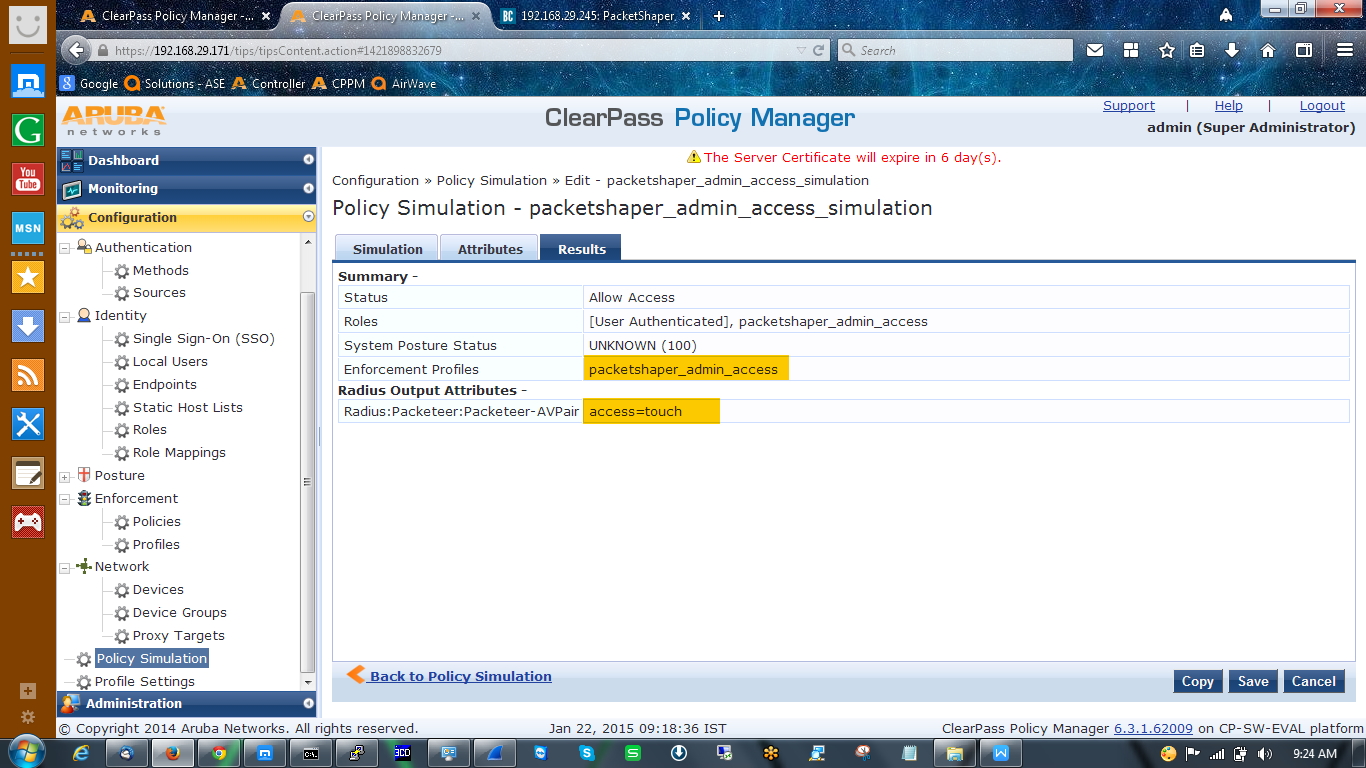




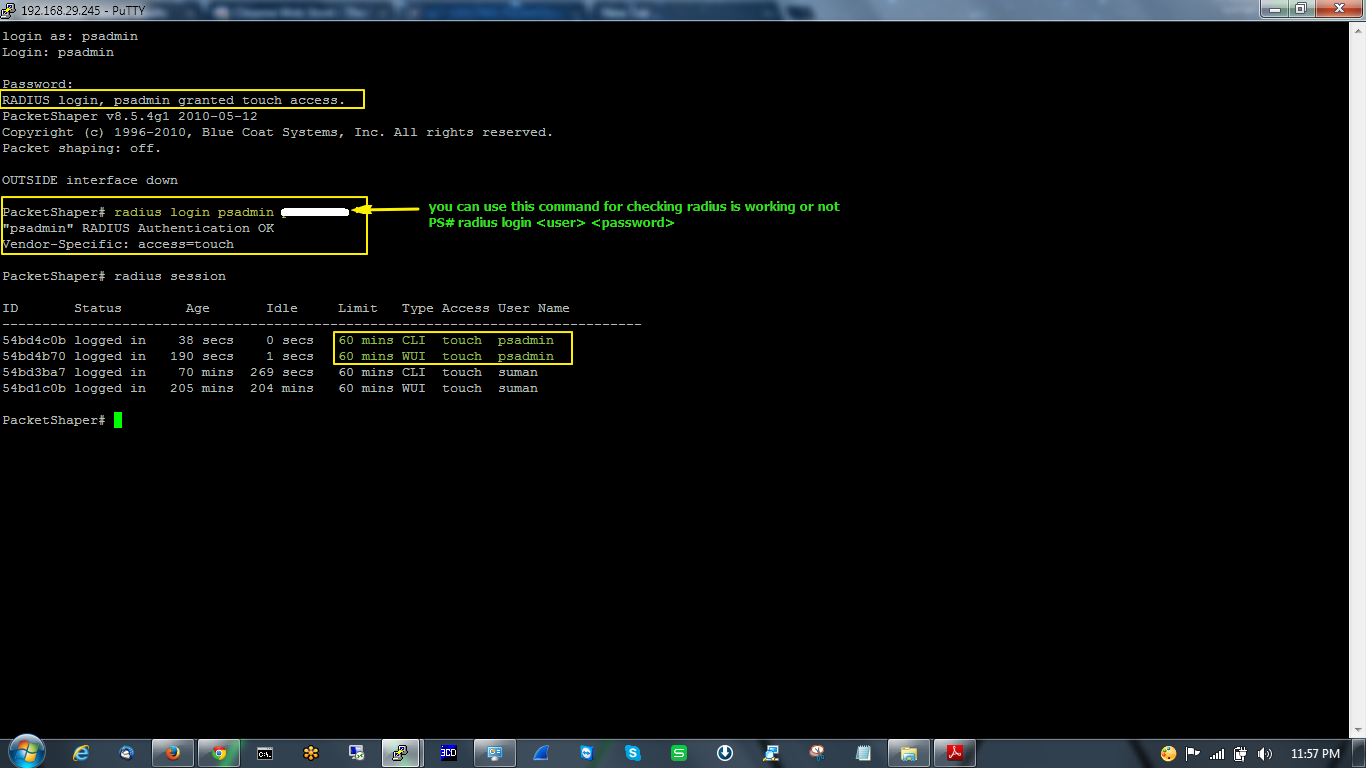


* **In Clearpass policy simulation.**





* **In Bluecoat Packetshaper.**



**THANK YOU**