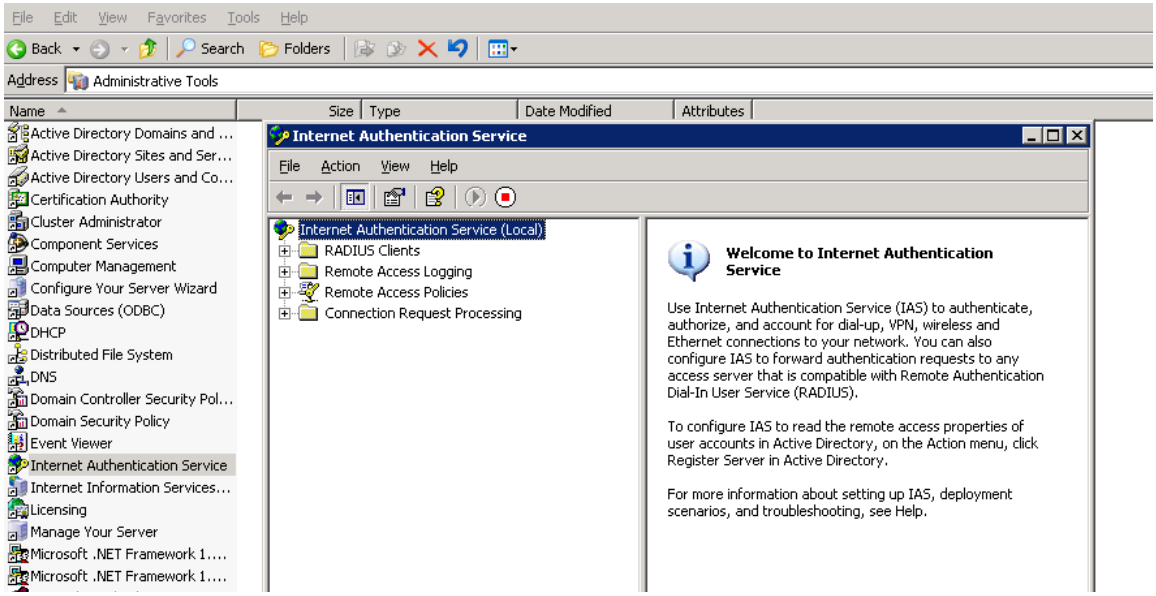
Management Authentication using Windows IAS as a Radius Server

OVERVIEW: In this we are using Radius server Windows IAS as a backend server for the management authentication for the controller. When the user try to login into the controller the request will first go to the external radius server to validate. If the user entry is present in the Windows AD(Active Directory) the success authentication will happen and the user can login into the controller with the admin rights.
We are using this technique as to provide more security within the network, i.e. only valid users those have a privilege can access the network device.

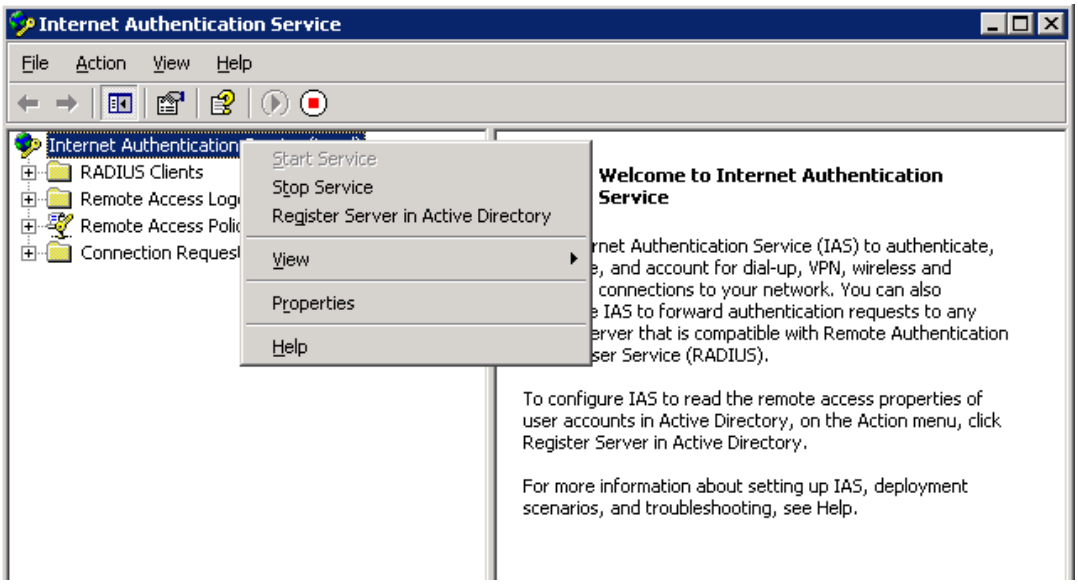
Q: **What are the settings I have to configure on the controller as well as on the radius server for successful management authentication and bypass the enable password?**

First of all we have to configure an external radius server (IAS). Please do the below steps to configure the radius server.

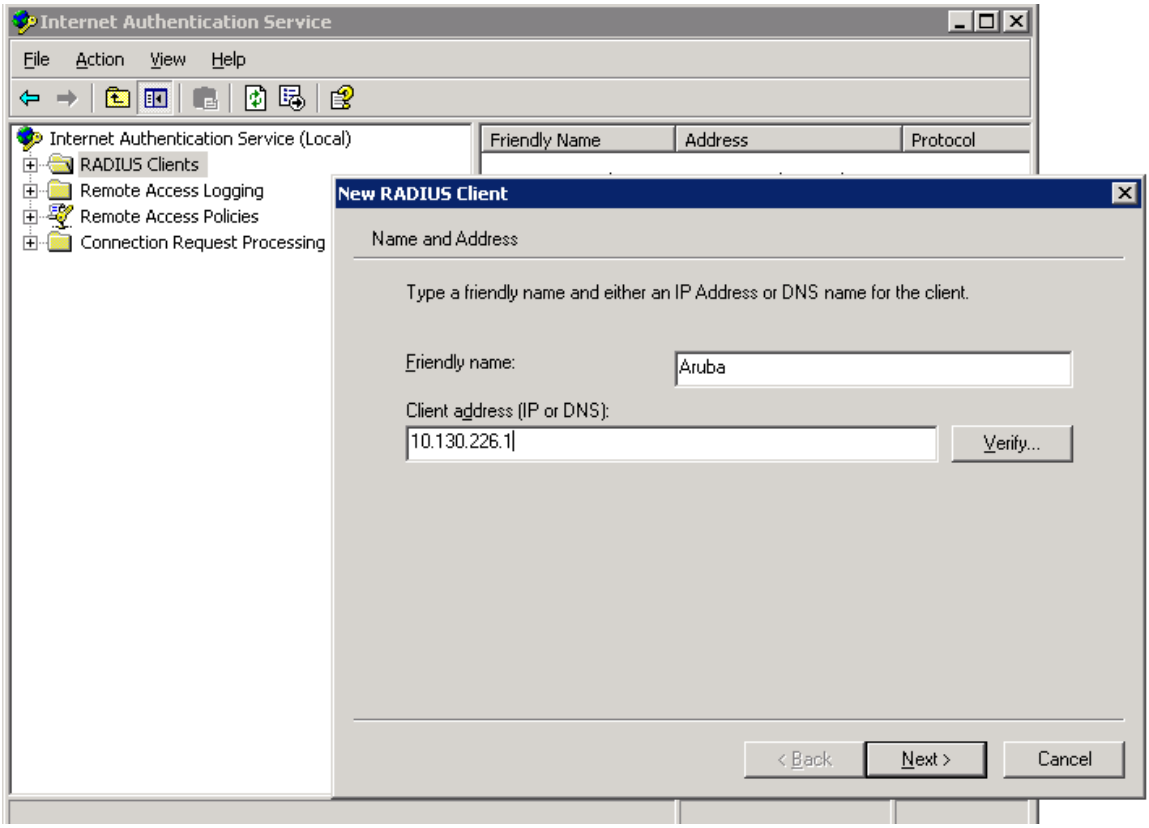
Please navigate to Start -> Settings -> Control Panel -> Administrative Tools -> Internet Authentication Service ->click



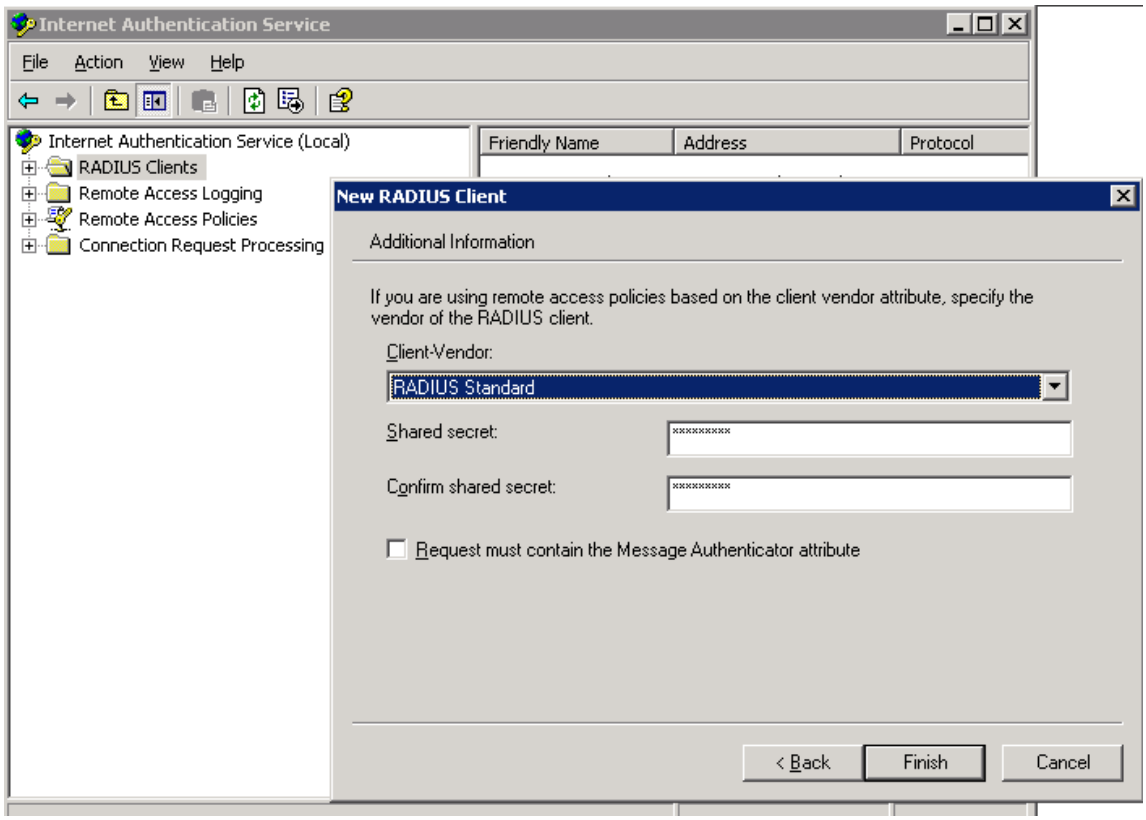
Right click on the Internet Authentication Service(local) and check whether the service is start or not. If not please start the service.



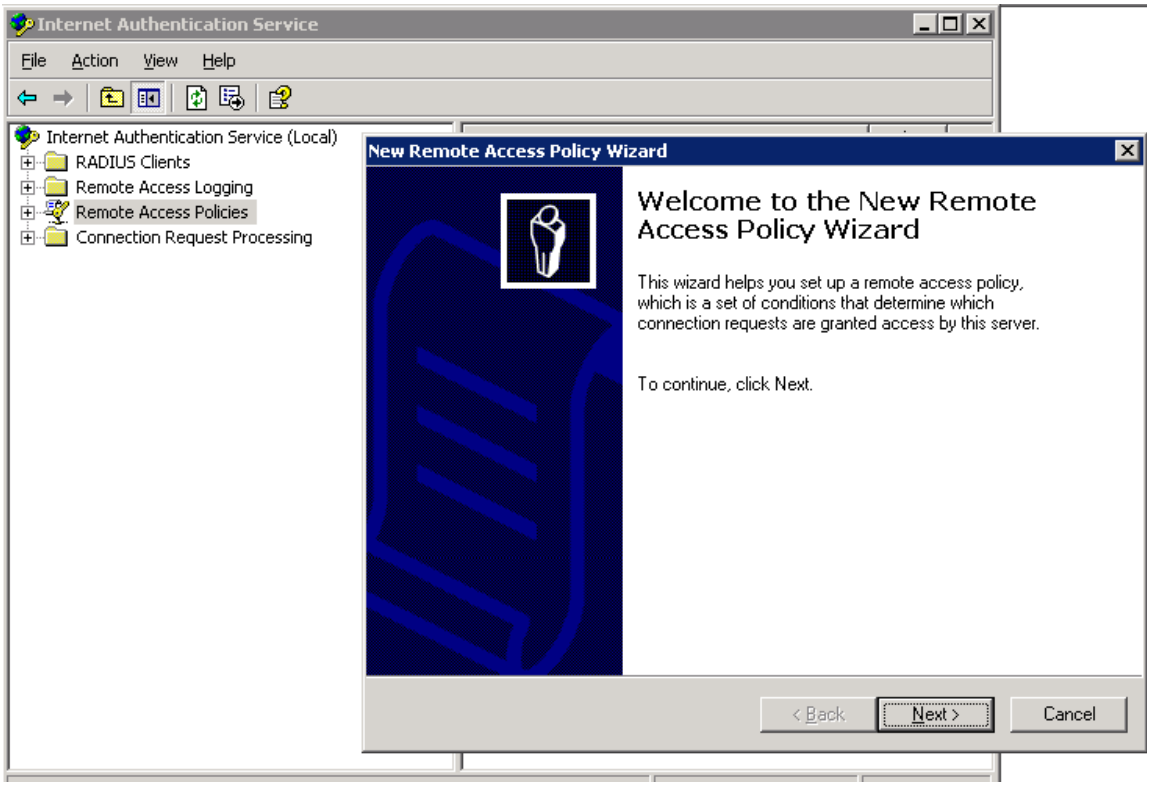
Right click on the "Radius Clients" and select New Radius Client. Specify any friendly name to the radius client and below mention the controller's IP address or Switch IP address. Click on next button.



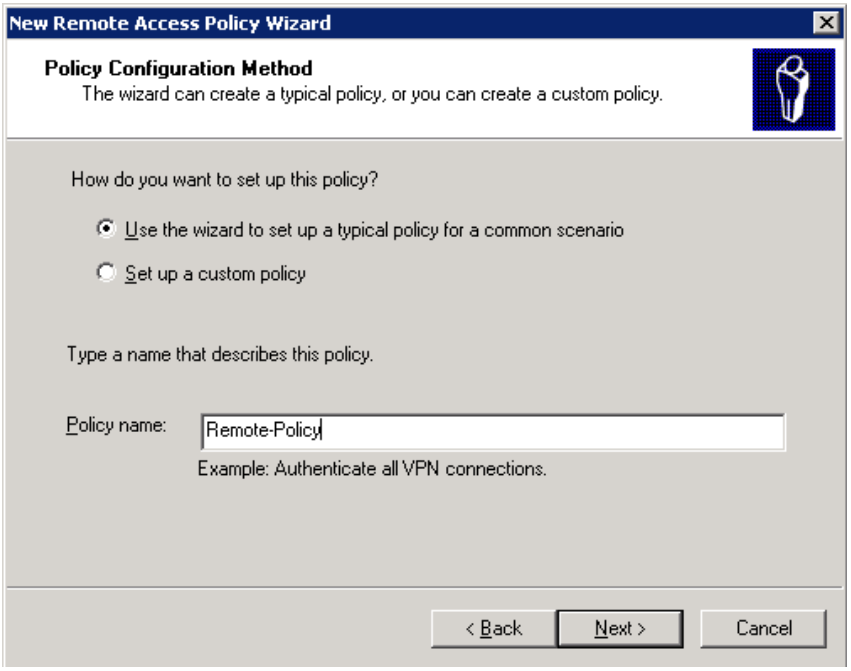
Specify the Shared Secret key in the below screen (in my case its "aruba@123") and click the finish button.



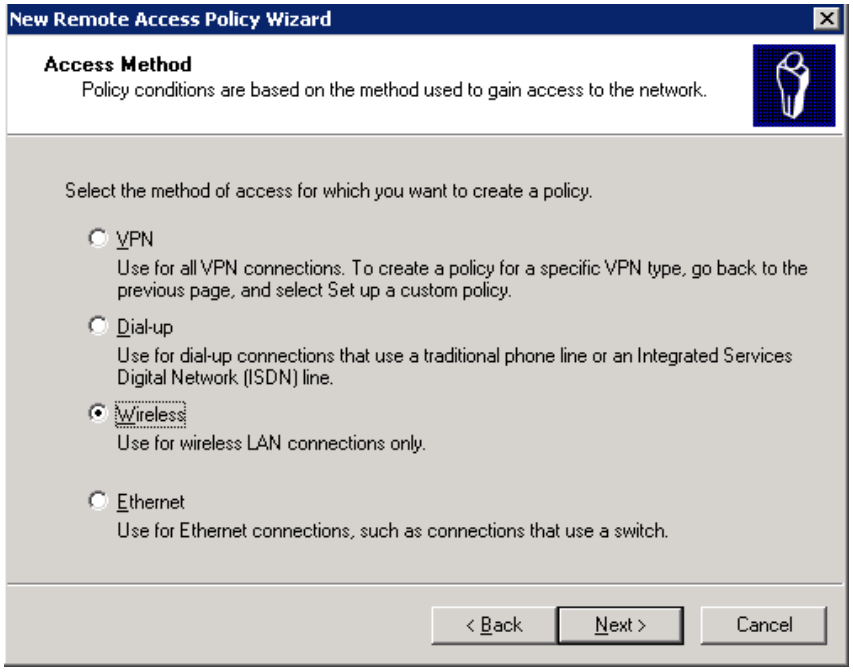
Now create the remote policy, right click on the “Remote Access Policies” and select “New Remote Access Policy” the below screen will appears. Lick on the next button



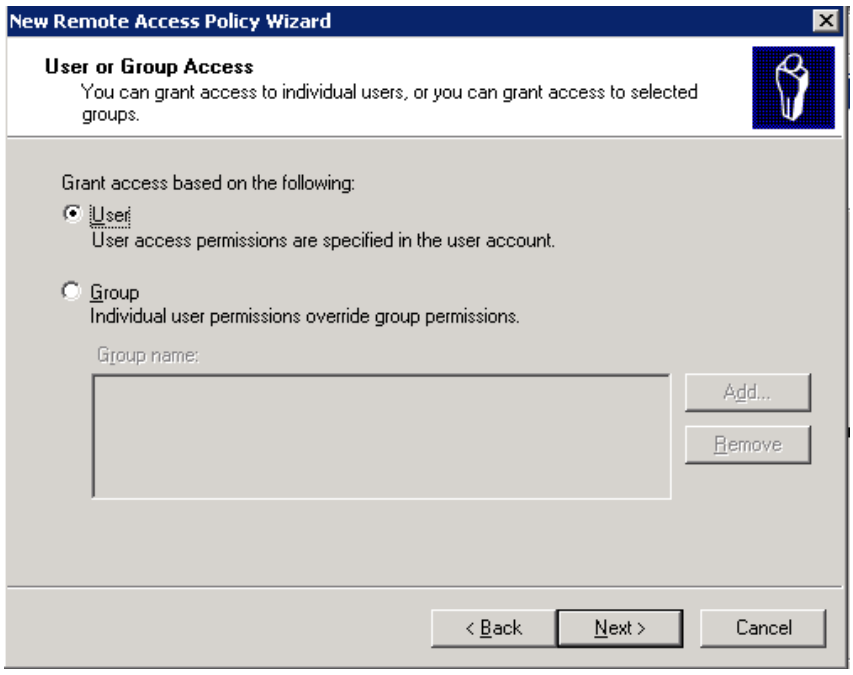
Select the first option “Use the wizard to set up” and give some name to the remote policy e.g. Remote-Policy. Click on the next button



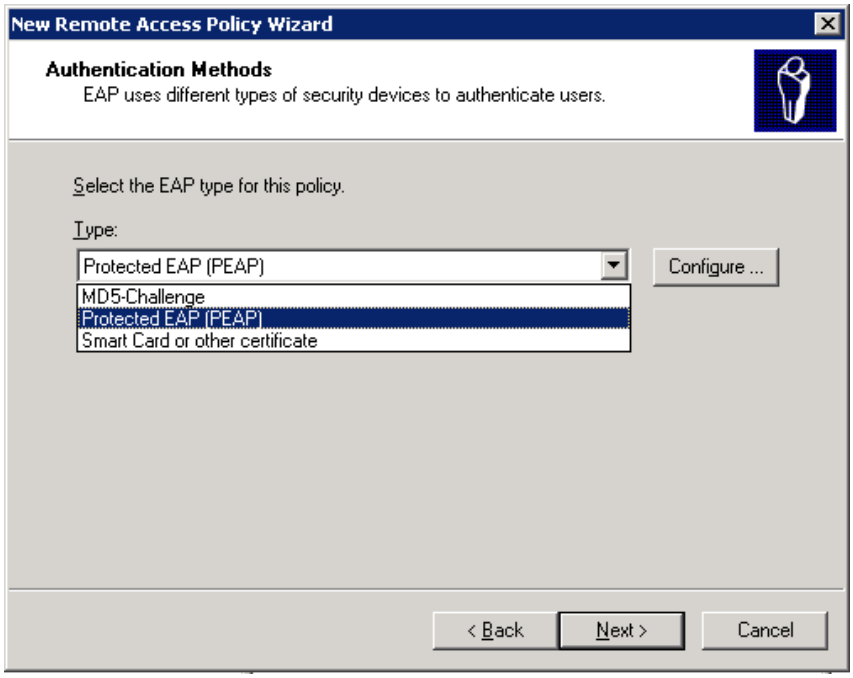
Select the options based on the method used to gain access to the network. In our case I am using Wireless. Click on next button



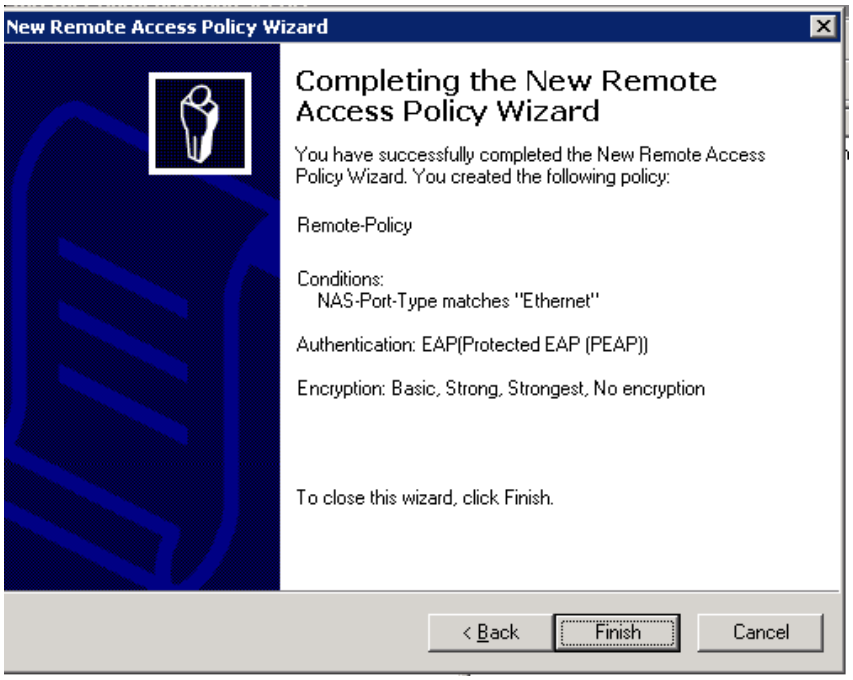
Select the user or group in the below screen. In my scenario I am using the user instead of group. Click on the next button.



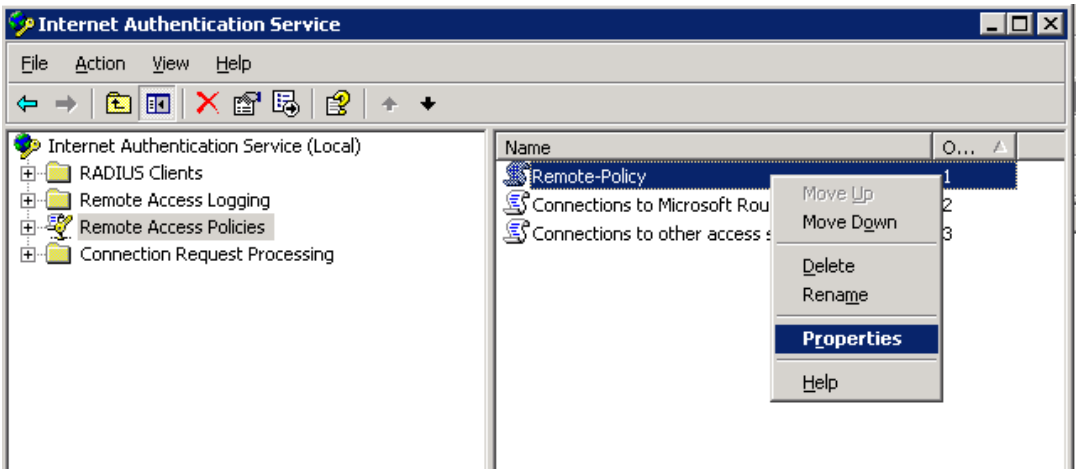
Select the Protected EAP (PEAP) from the drop down menu and click on the next button.



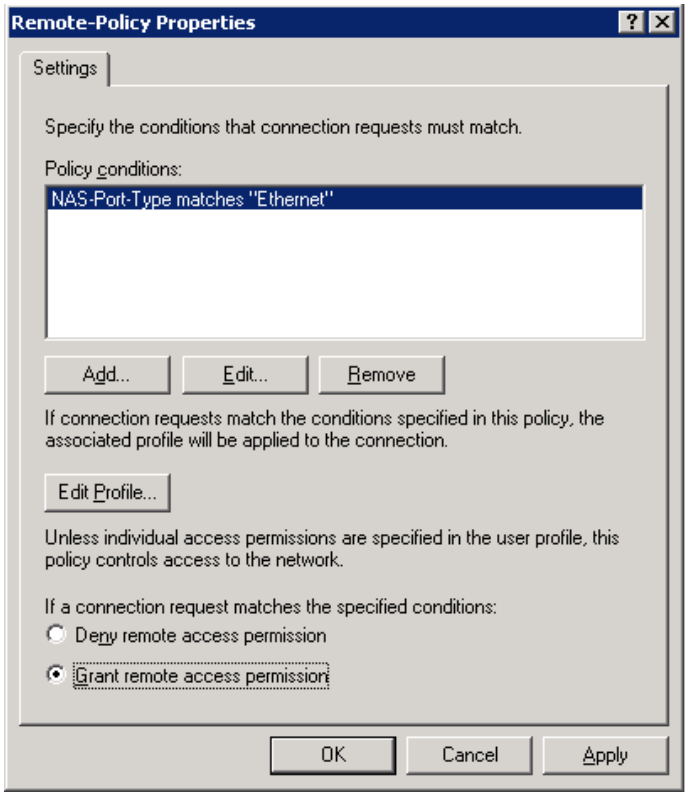
Click on the finish button to save the changes.



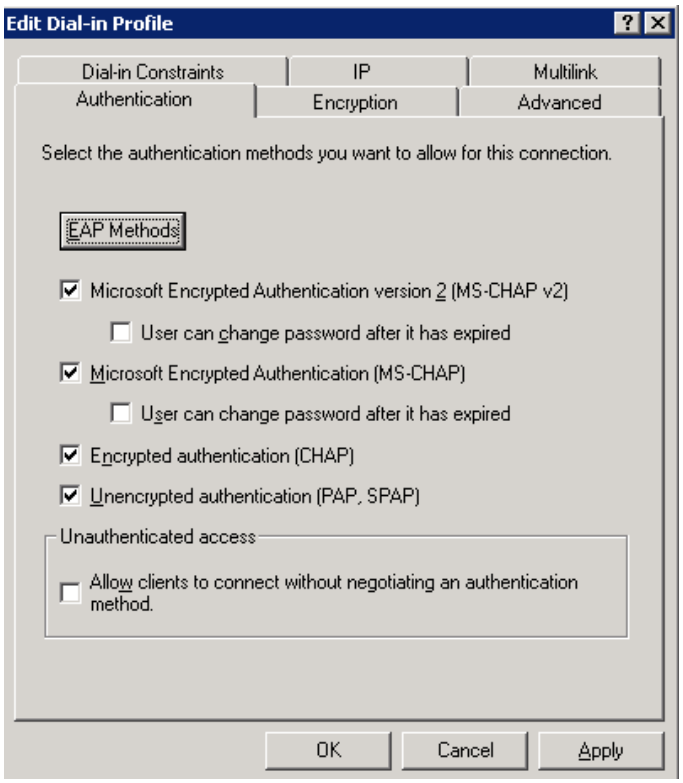
Right click on the Remote policy we have created just now and go to the properties.



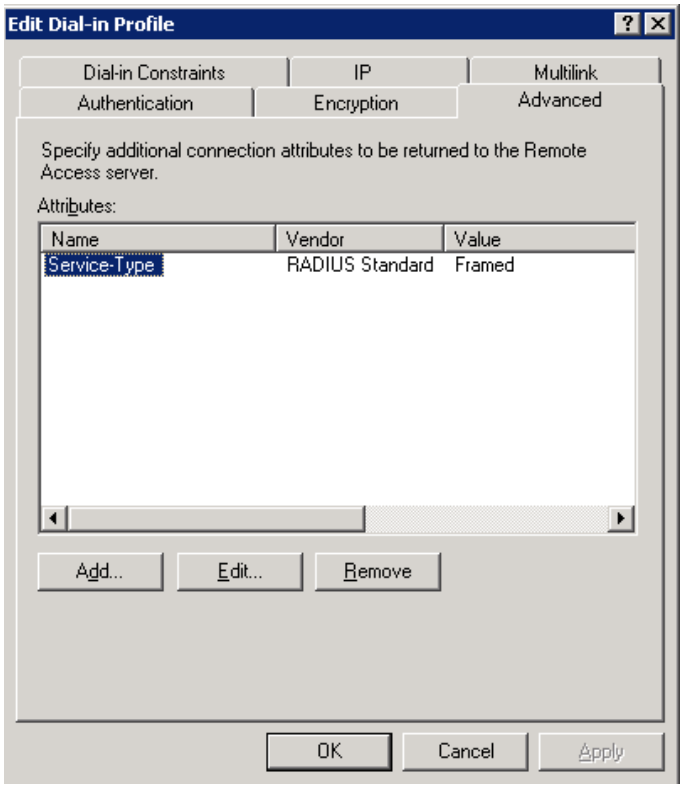
The below window will open. Choose the Grant remote access permission option and click on “Edit Profile”



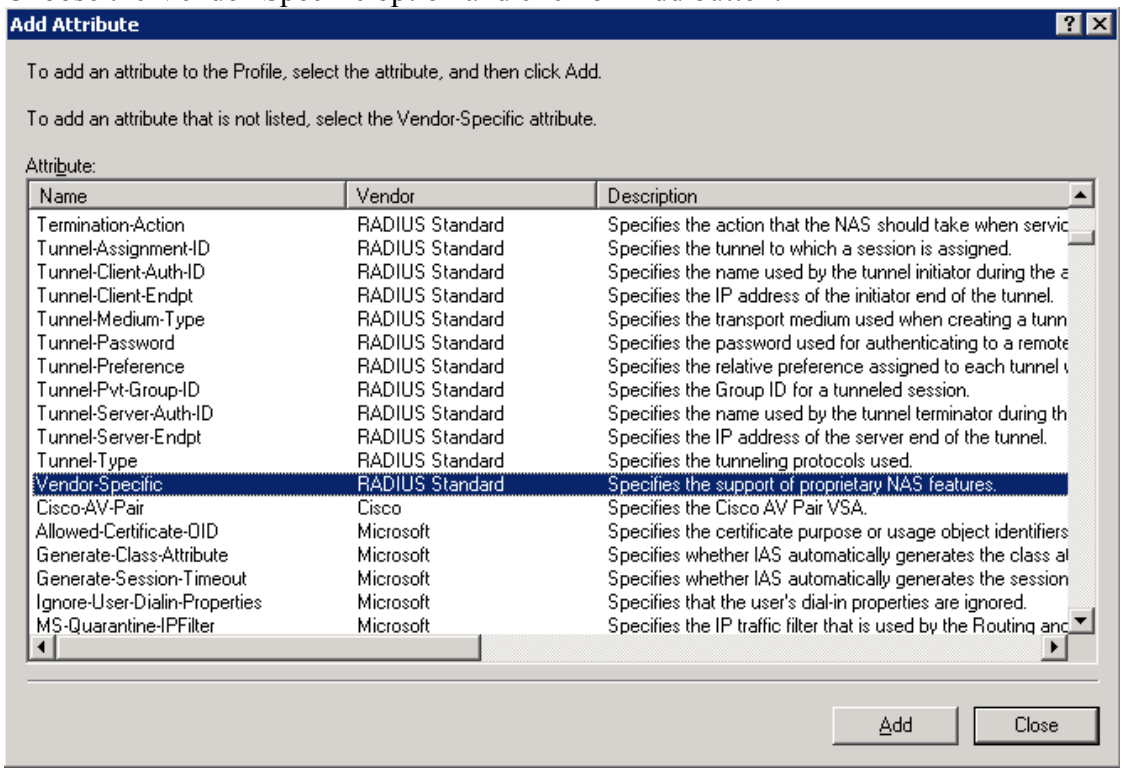
Click on the Authentication tab and select the below authentication method that includes PAP and MSCHAP. Click on the Apply button to save the changes.



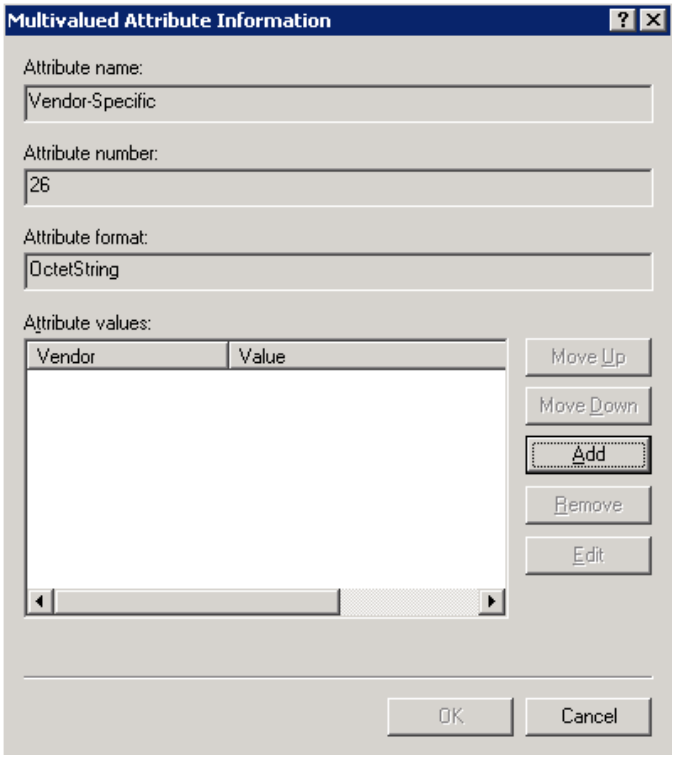
Click on the Advanced tab on the same window as above. Click on the add button



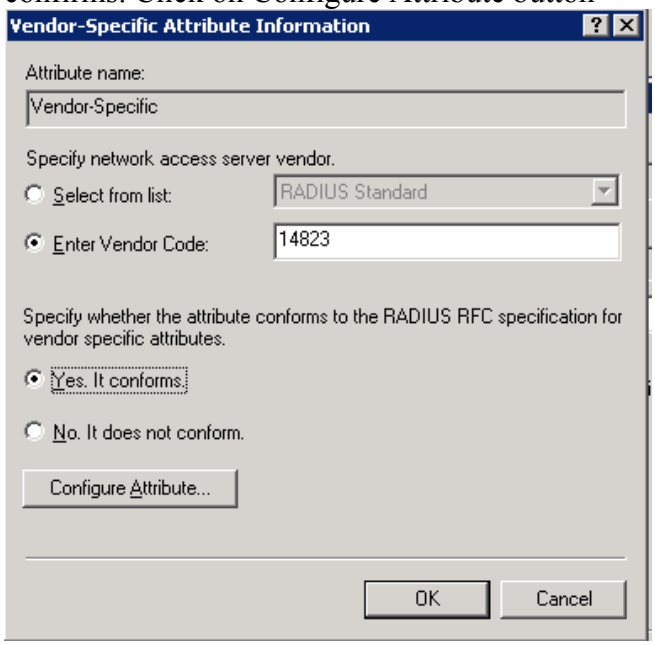
Choose the Vendor-Specific option and click on Add button.



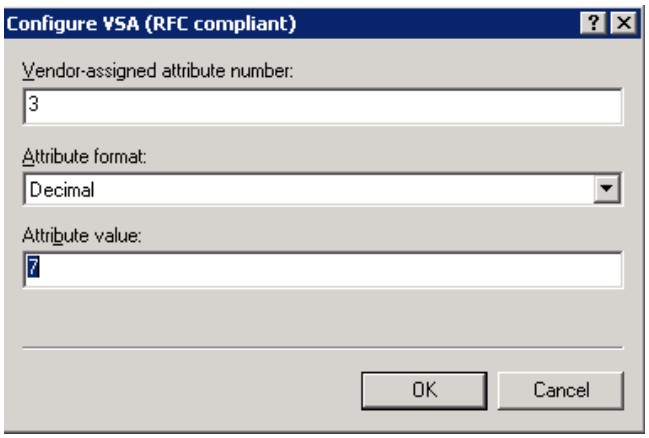
Click on the add button in the below window



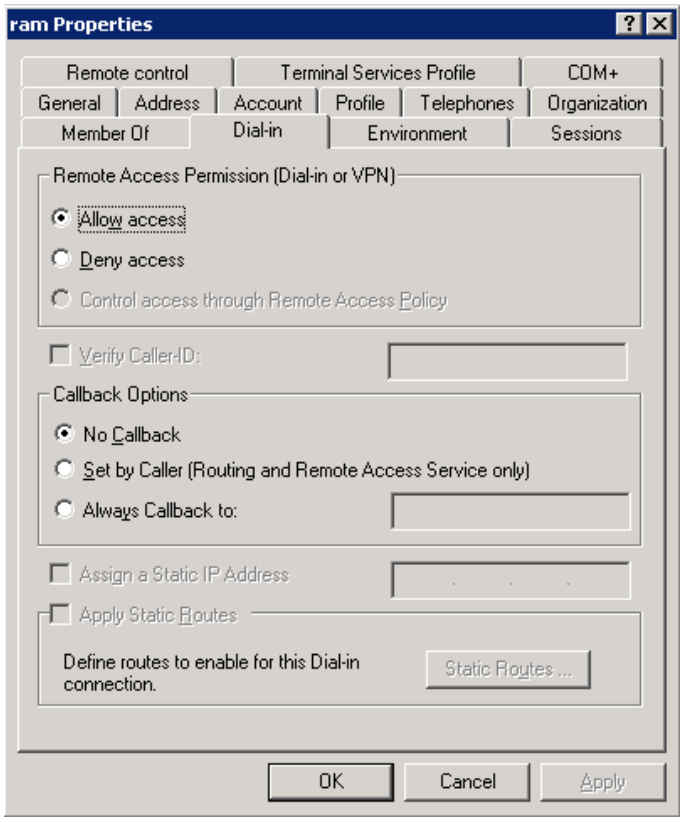
Enter the vendor code as 14823(which is for Aruba) and choose the option Yes, It confirms. Click on Configure Attribute button



Specify the Vendor-assigned attribute number as 3 and attribute value as 7 and click on Ok button to save the changes.



Click on Ok and apply buttons in all the windows as to save the changes. Also create a user entry in the active directory. After creating the user entry on the Windows Active directory, right click on the user and go to the properties. Select the Dial-in tab and choose the “Allow access” for the user and click on Ok button.

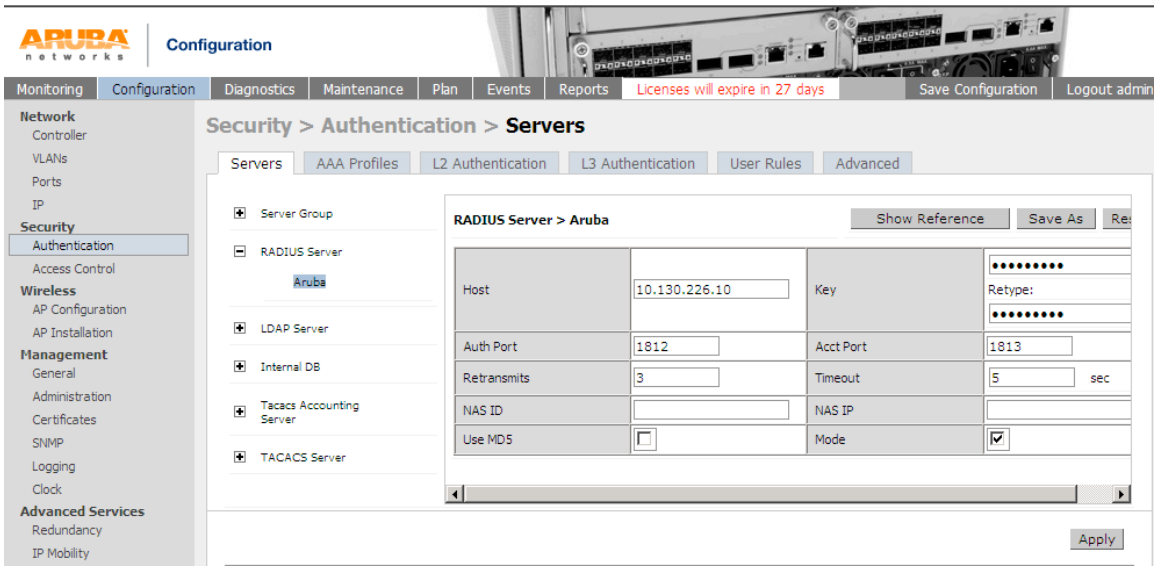


The setting we have to configure on the Aruba controller or Switch.

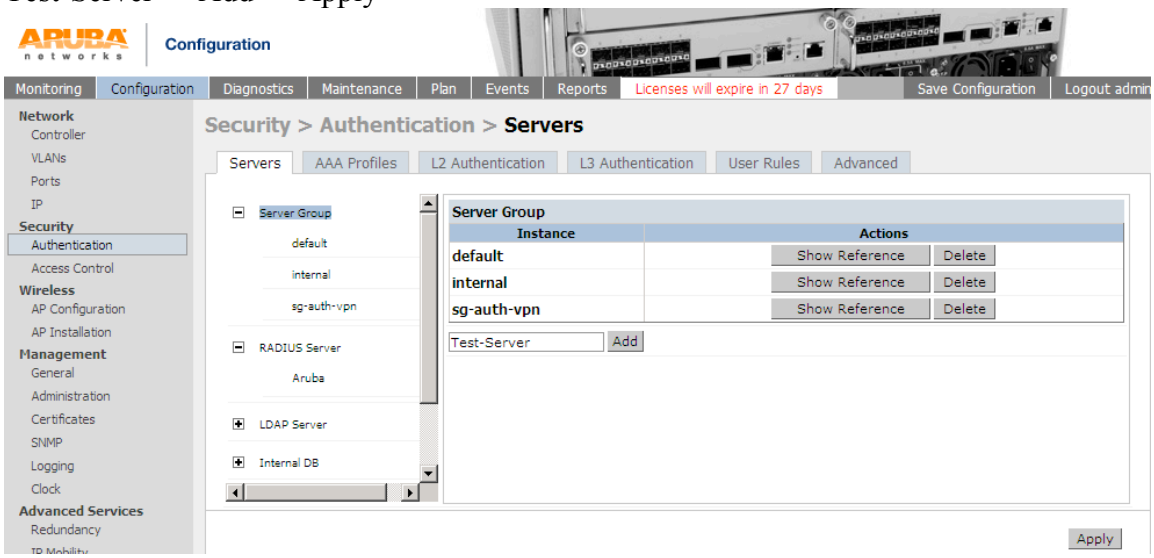
FROM WEBUI:

Please navigate to Configuration tab-> Under Security click on Authentication -> Select the Servers tab -> Click on RADIUS Server -> Specify any name e.g. Aruba -> add -> Apply

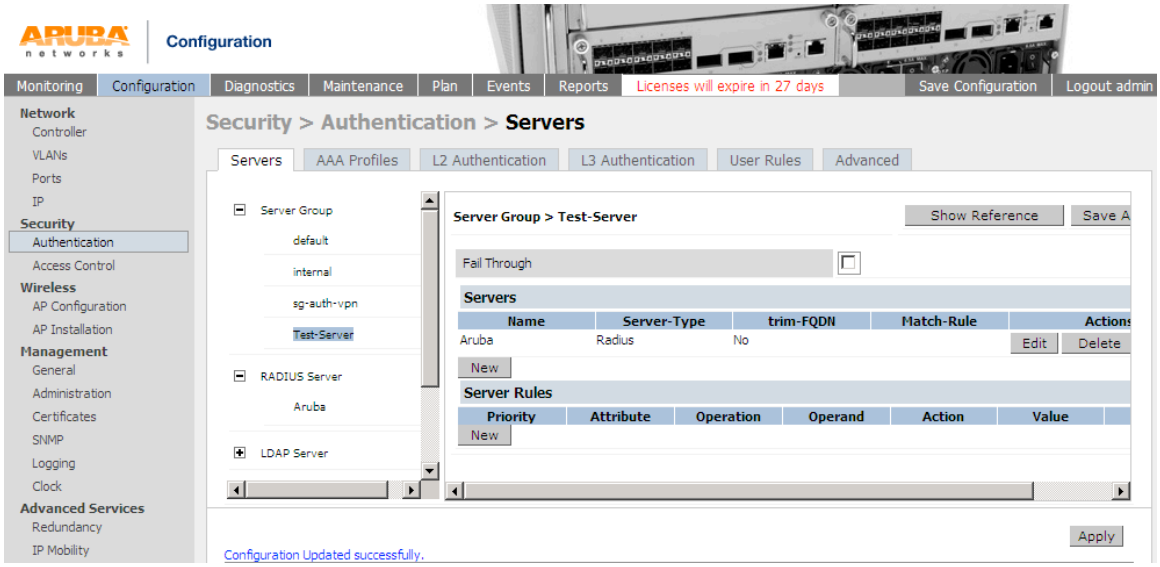
Click on the Radius server you just created and specify the details like radius client ip address and the shared secret key -> Apply



Click on the Server Group under the same window and create a new server group e.g. Test-Server -> Add -> Apply

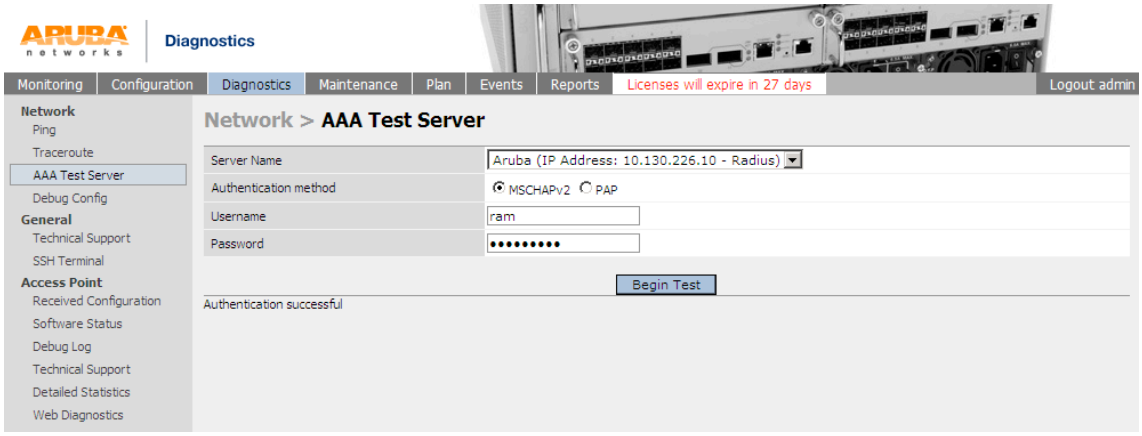


Choose the Server Group you created above -> on the RHS click on new button choose the radius server from the drop down menu -> Add Server -> Apply

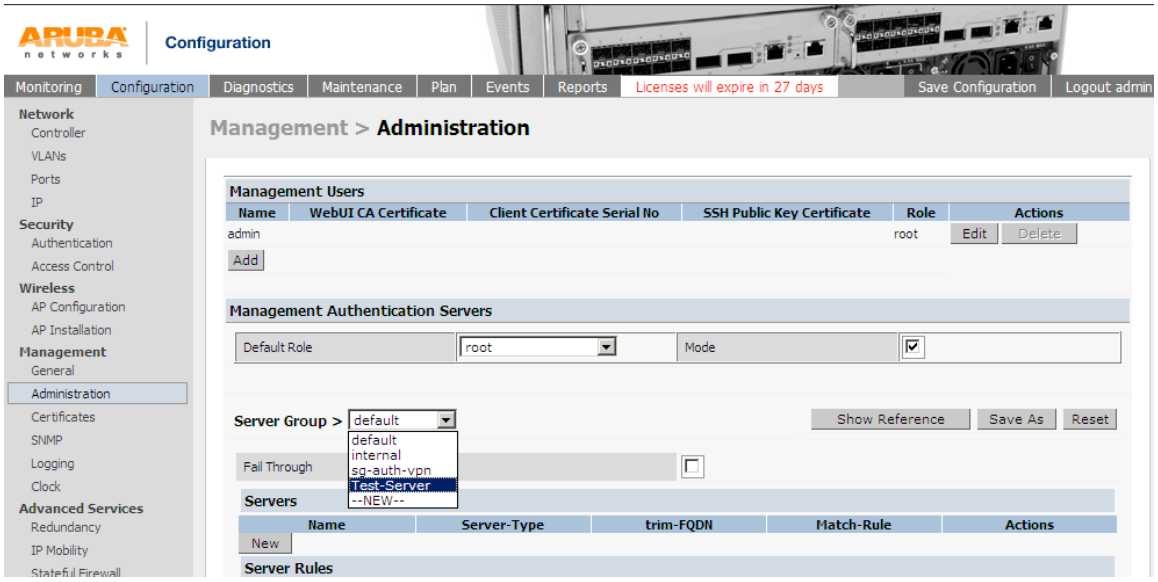


As to check whether the communication is happens between Aruba Controller and radius server. Go to Diagnostics tab -> AAA test server -> From the drop down menu select the radius server e.g. Aruba -> choose any authentication method PAP or MSCHAPv2-> Specify the username -> type the password -> Begin test

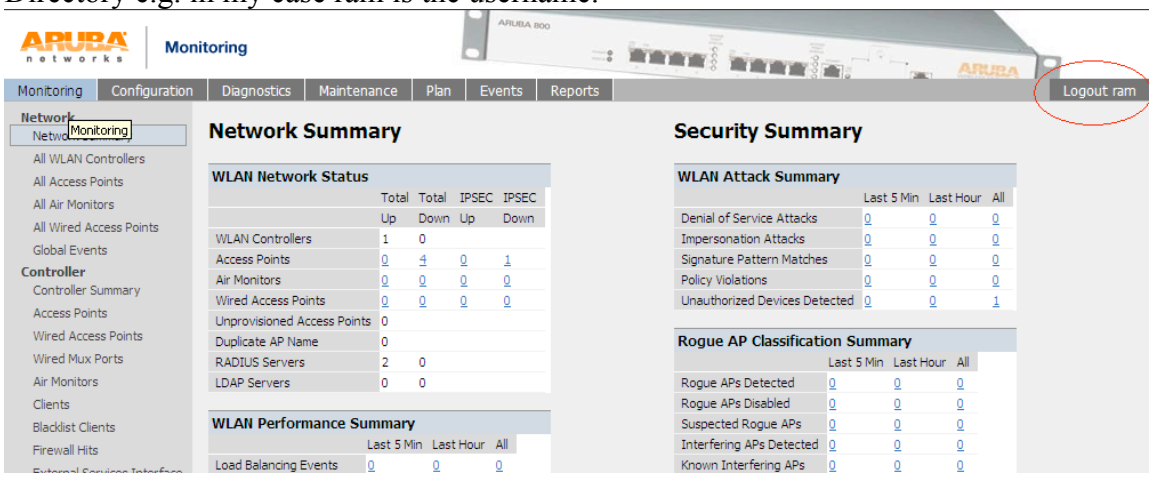
If you will see the Authentication successful means communication happens between Aruba controller and Radius server.



Please navigate to Configuration tab-> Under Management click on Administration -> On the RHS select the server group under Management Authentication Servers from the drop-down menu e.g. Test-Server-> Apply



Try to login into the controller with the user entry present on the Windows Active Directory e.g. in my case ram is the username.



FROM CLI:

(Aruba) #configure t
Enter Configuration commands, one per line. End with CNTL/Z

(Aruba) (config) #aaa authentication-server radius **Aruba**
(Aruba) (RADIUS Server "Aruba") #enable
(Aruba) (RADIUS Server "Aruba") #host **10.130.226.10**
(Aruba) (RADIUS Server "Aruba") #key **aruba@123**
(Aruba) (RADIUS Server "Aruba") #exit
(Aruba) (config) #exit
(Aruba) #aaa test-server pap Aruba ram aruba@123

Authentication successful

(Aruba) #show aaa authentication-server all

Auth Server Table

Name	Type	IP addr	AuthPort	Status	Inservice	Requests
Internal	Local	10.130.226.4	n/a	Enabled	Yes	0
Aruba	Radius	10.130.226.10	1812	Enabled	Yes	34

(Aruba) #

User: ram

Password: *********
NOTICE
NOTICE -- This switch has active licenses that will expire in 21 days
NOTICE
NOTICE -- See 'show license' for details.
NOTICE

(Aruba) #