

Management Authentication using Windows IAS as a Radius Server

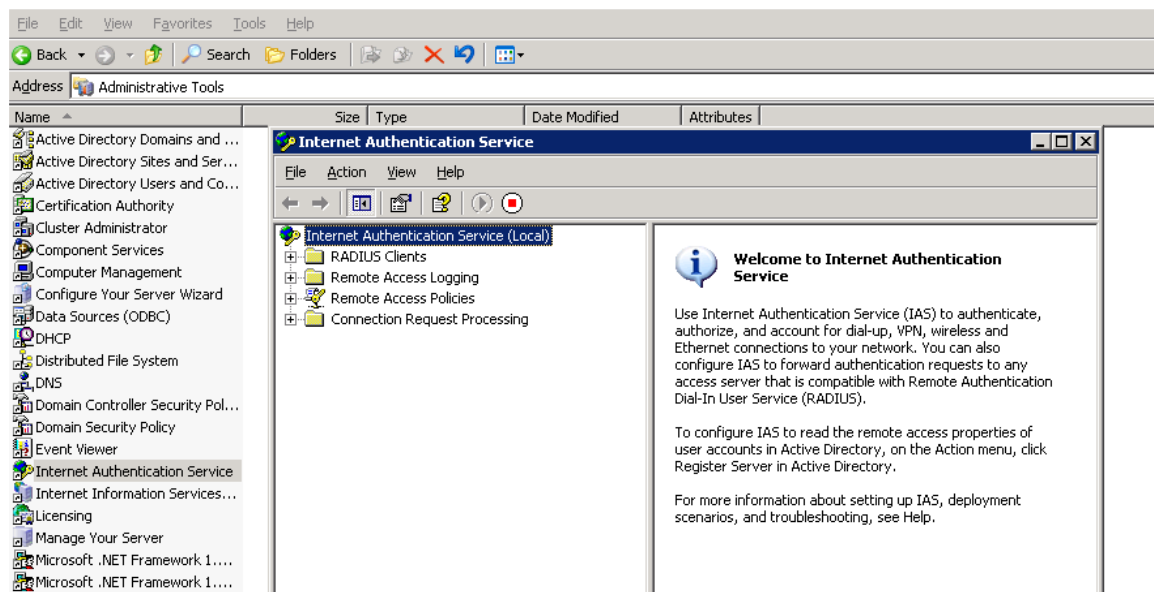
OVERVIEW: In this we are using Radius server Windows IAS as a backend server for the management authentication for the controller. When the user try to login into the controller the request will first go to the external radius server to validate. If the user entry is present in the Windows AD(Active 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.

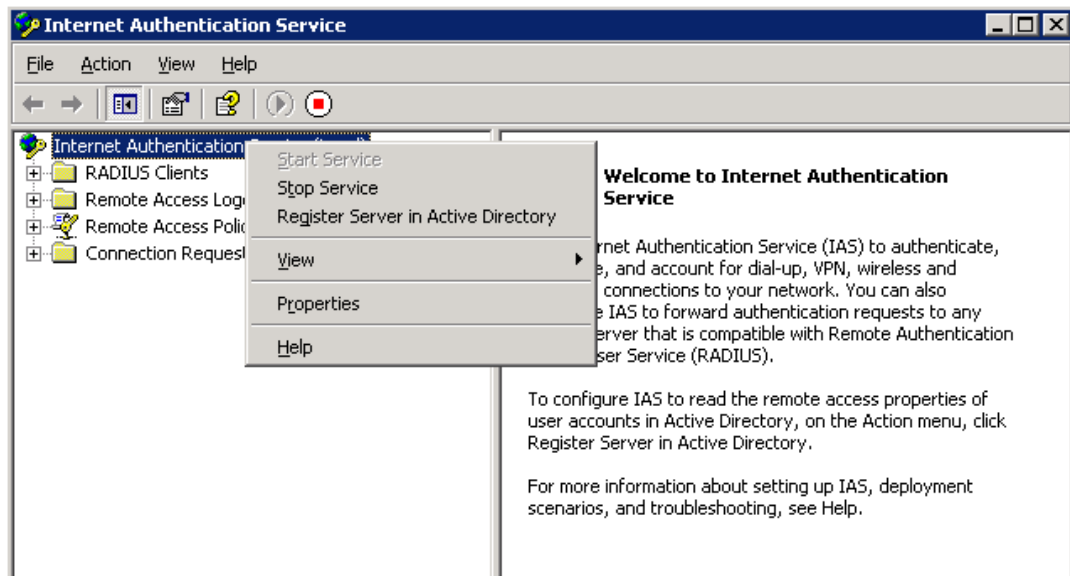
Q: What are the settings I have to configure on the controller as well as on the radius server for successful management authentication and bypass the enable password?

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

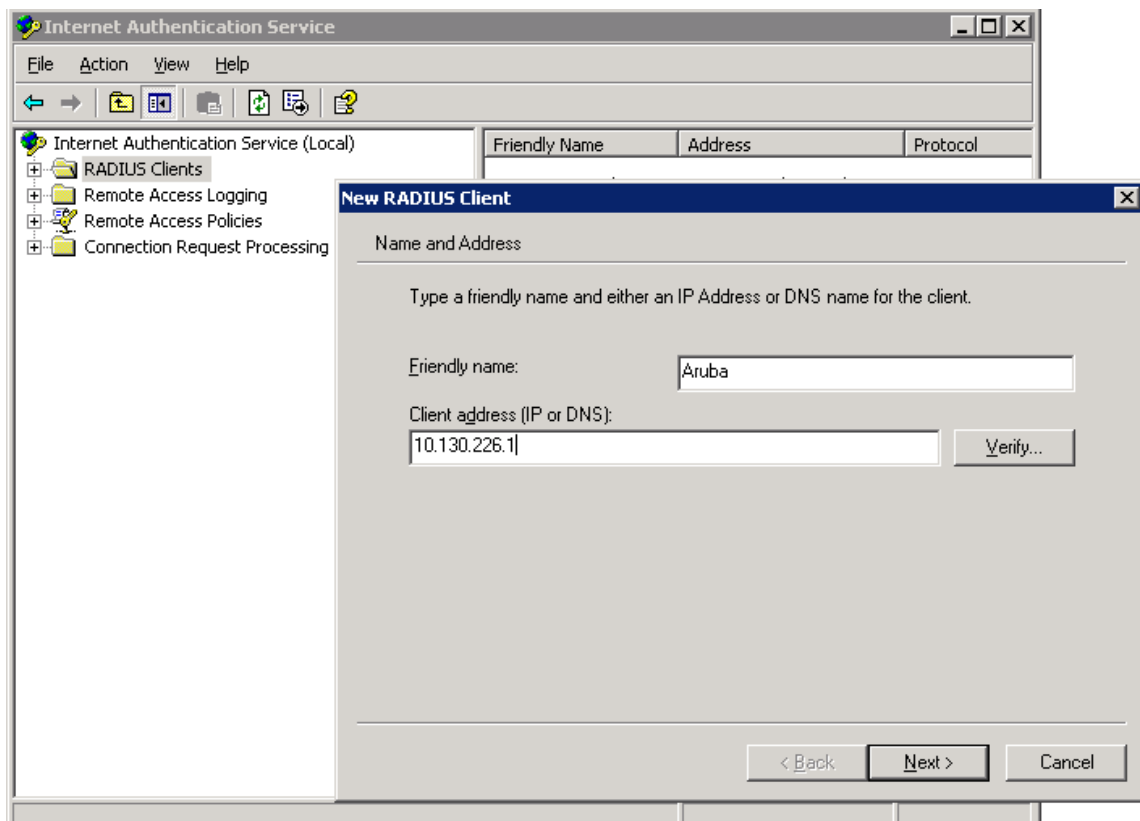
Please navigate to Start -> Settings -> Control Panel -> Administrative Tools -> Internet Authentication Service ->click



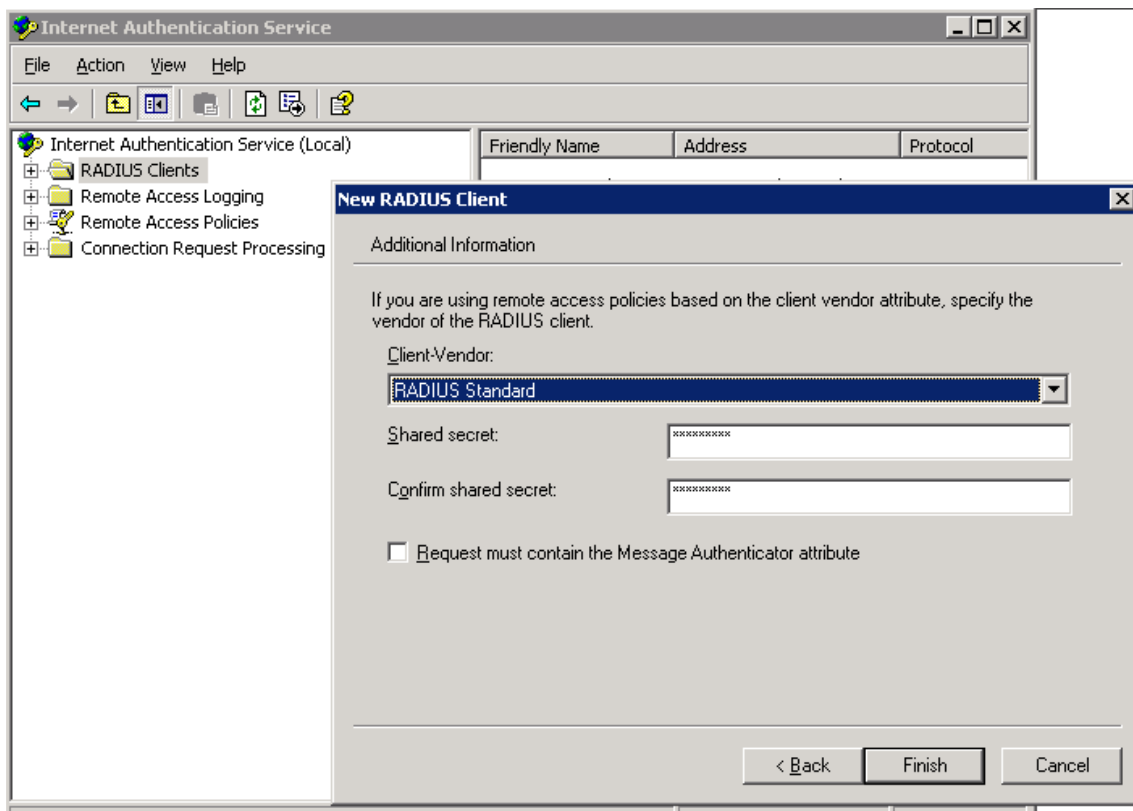
Right click on the Internet Authentication Service(local) and check whether the service is start or not. If not please start the service.



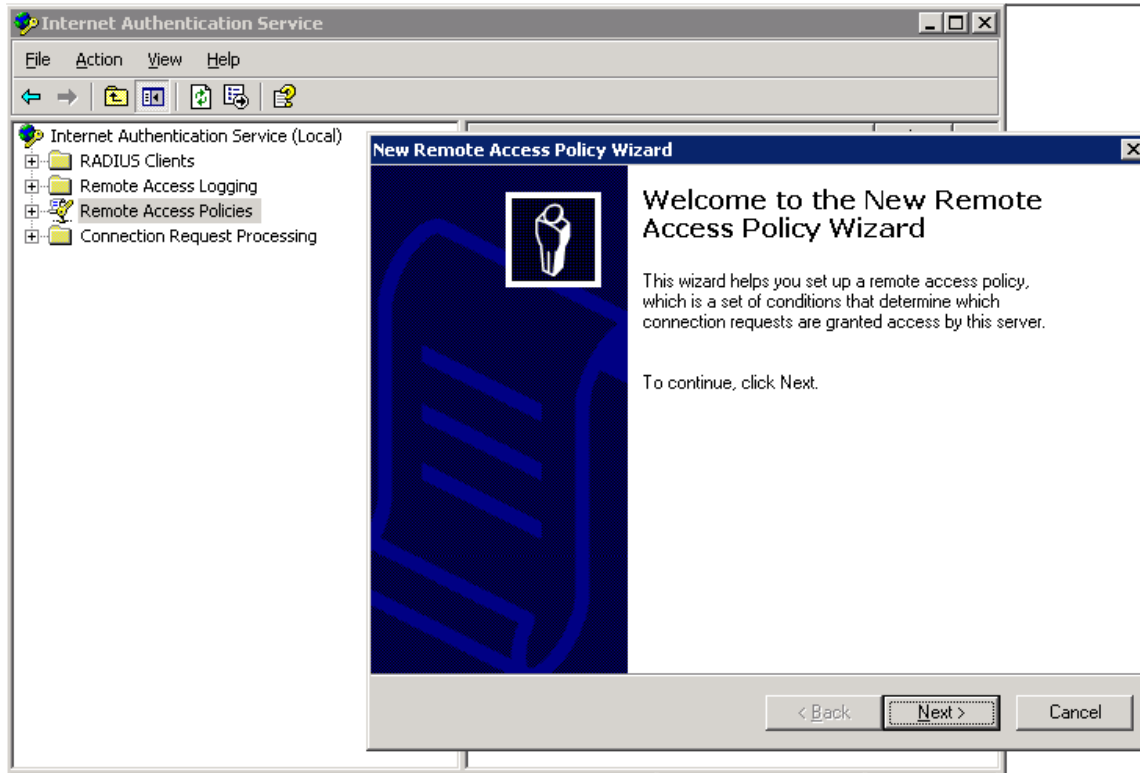
Right click on the “Radius Clients” and select New Radius Client. Specify any friendly name to the radius client and below mention the controller’s IP address or Switch IP address. Click on next button.



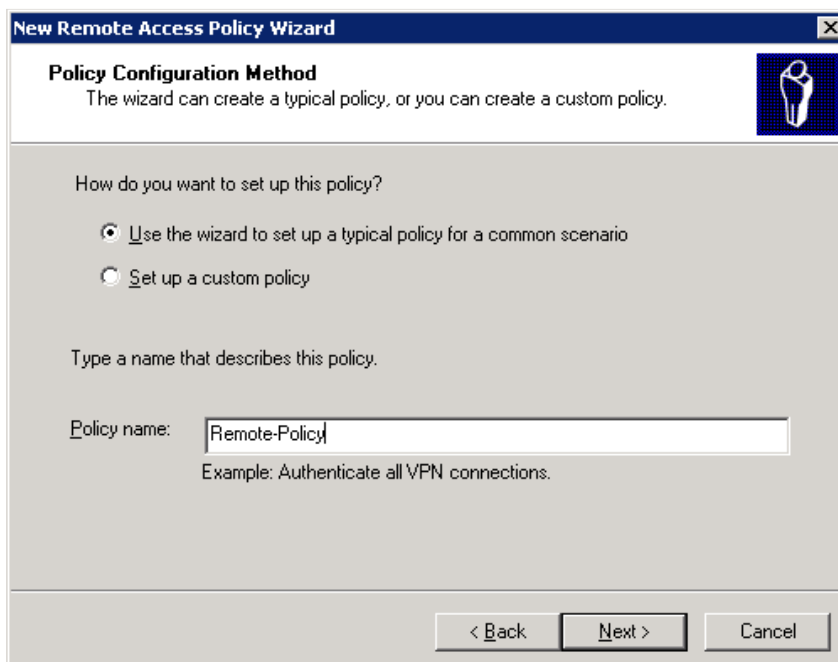
Specify the Shared Secret key in the below screen (in my case its “aruba@123”) and click the finish button.



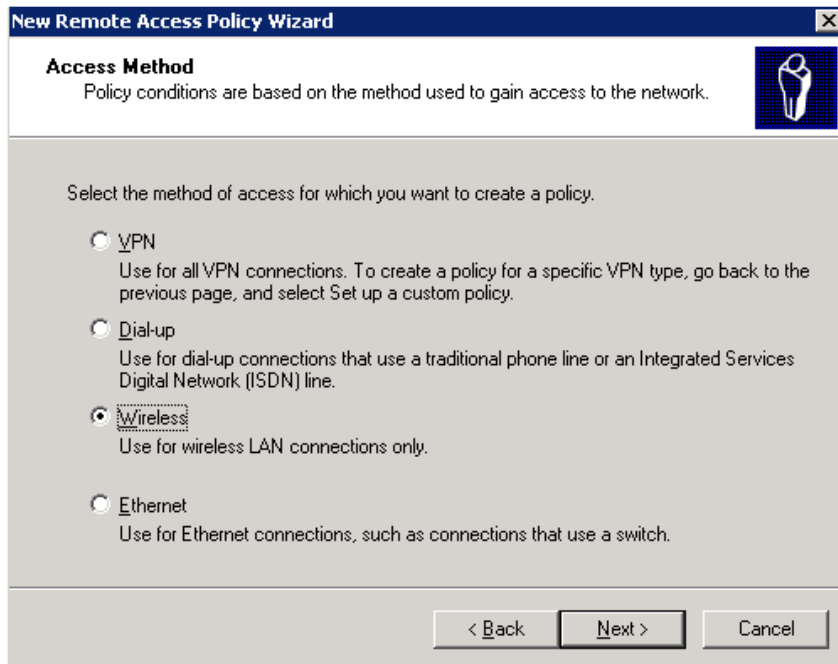
Now create the remote policy, right click on the “Remote Access Policies” and select “New Remote Access Policy” the below screen will appears. Lick on the next button



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



New Remote Access Policy Wizard

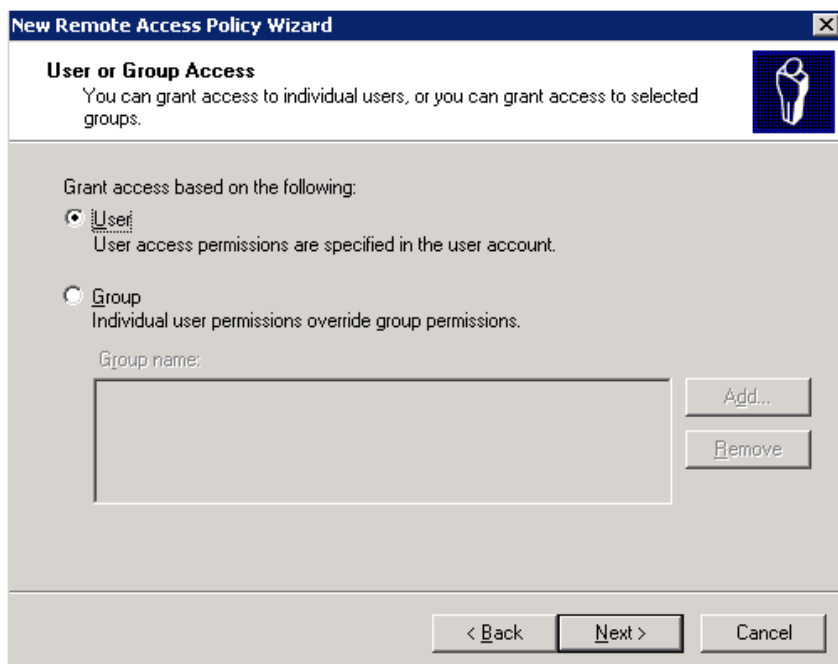
Access Method
Policy conditions are based on the method used to gain access to the network.

Select the method of access for which you want to create a policy.

- ☐ **V**PN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.
- ☐ **D**ial-up
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
- ☒ **W**ireless
Use for wireless LAN connections only.
- ☐ **E**thernet
Use for Ethernet connections, such as connections that use a switch.

< Back Next > Cancel

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.



New Remote Access Policy Wizard

User or Group Access
You can grant access to individual users, or you can grant access to selected groups.

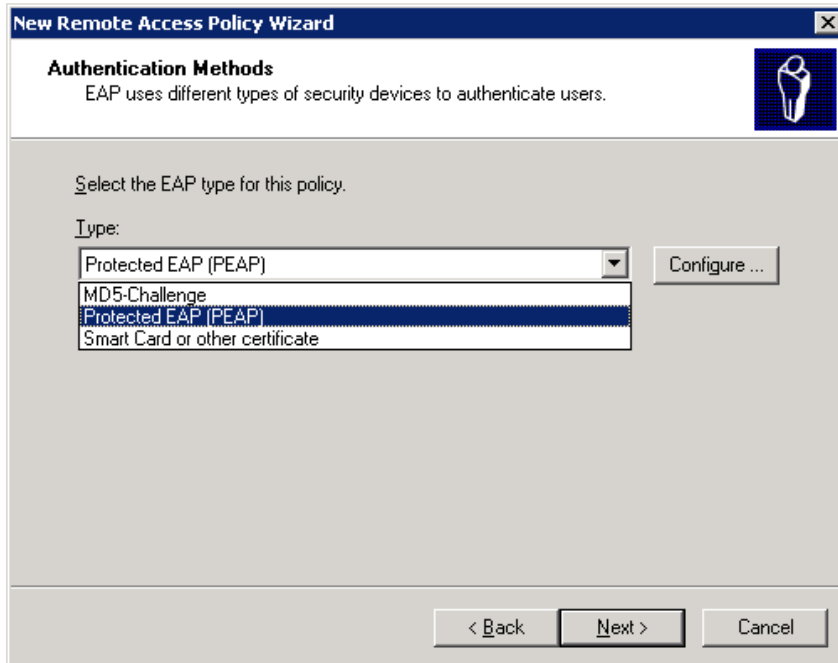
Grant access based on the following:

- ☒ **U**ser
User access permissions are specified in the user account.
- ☐ **G**roup
Individual user permissions override group permissions.
Group name:

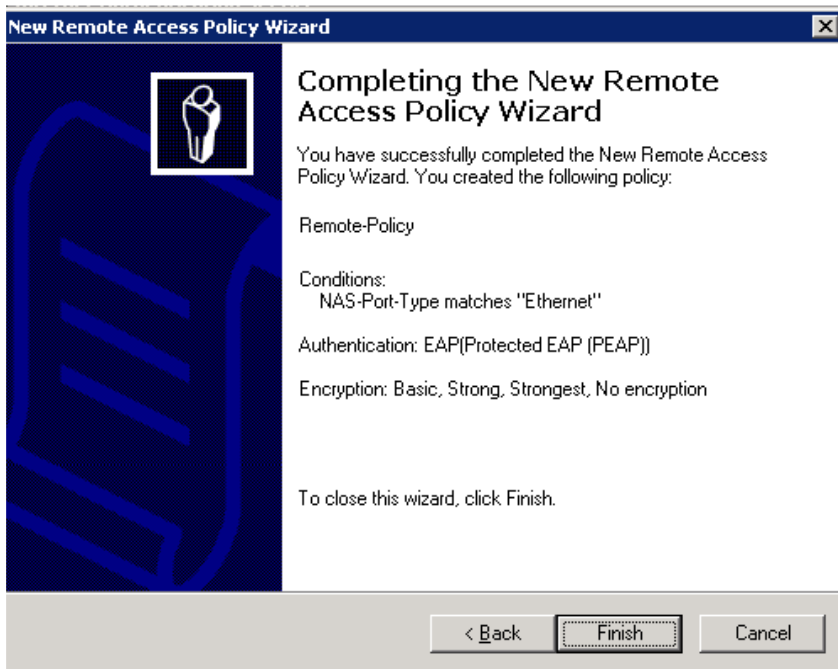
Add...
Remove

< Back Next > Cancel

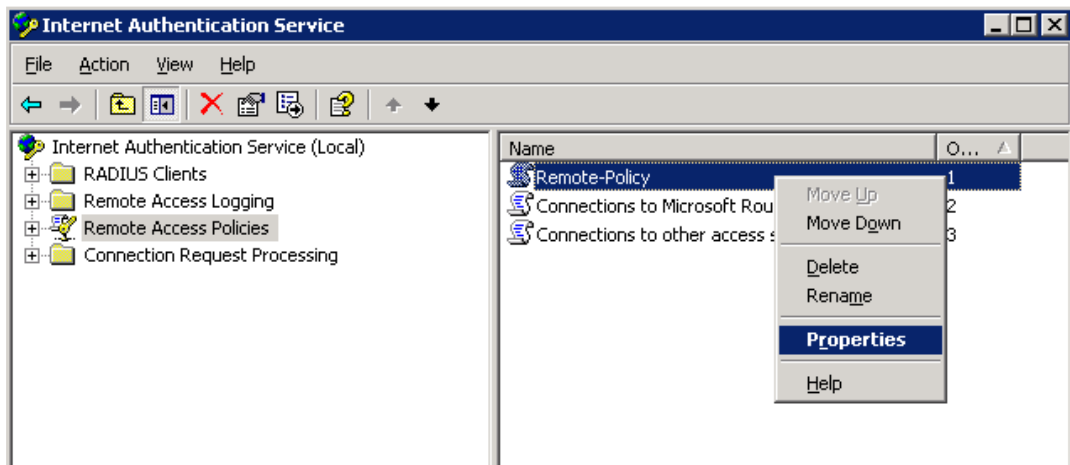
Select the Protected EAP (PEAP) from the drop down menu and click on the next button.



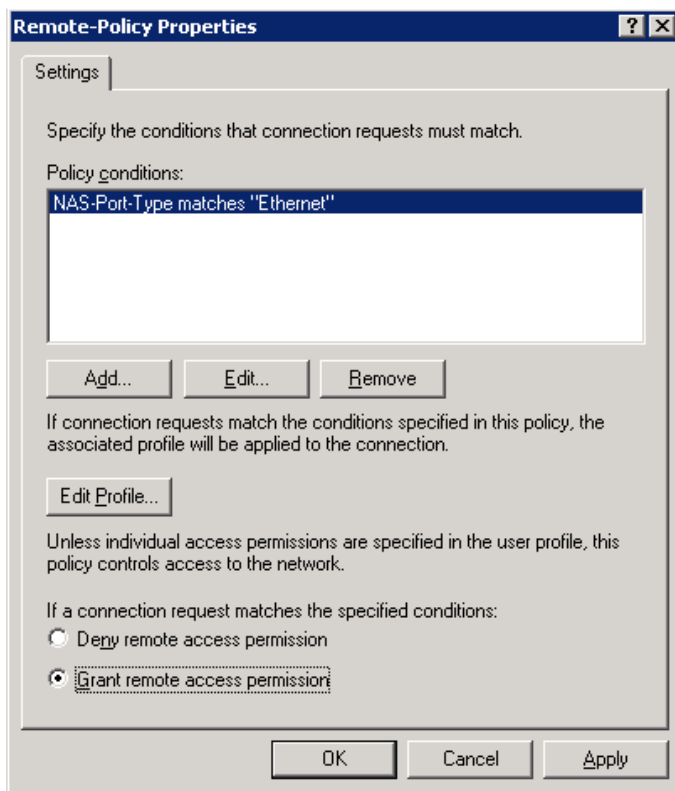
Click on the finish button to save the changes.



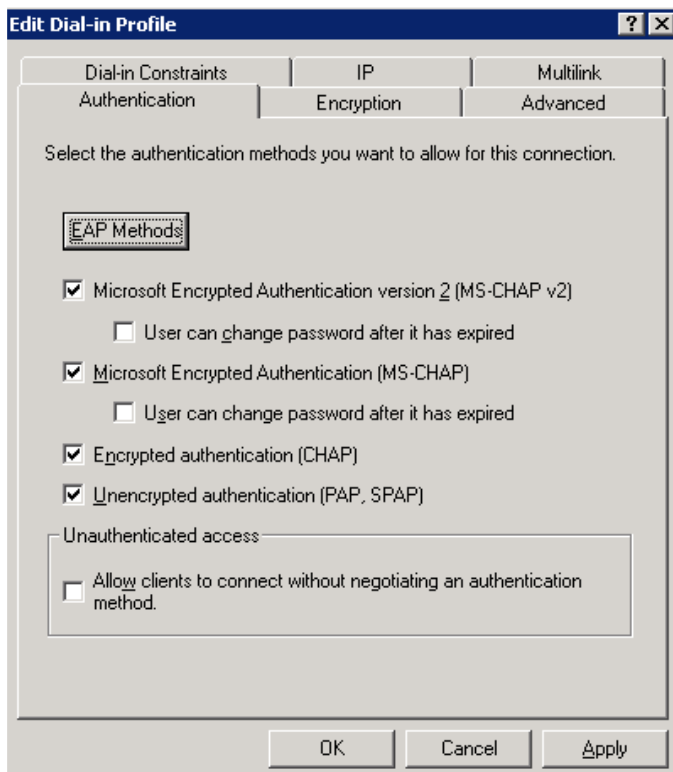
Right click on the Remote policy we have created just now and go to the properties.



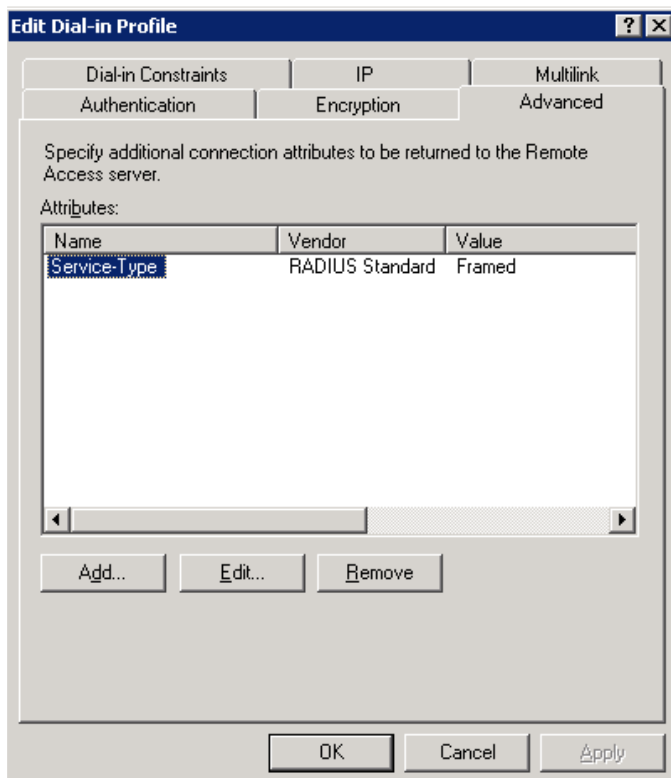
The below window will open. Choose the Grant remote access permission option and click on “Edit Profile”



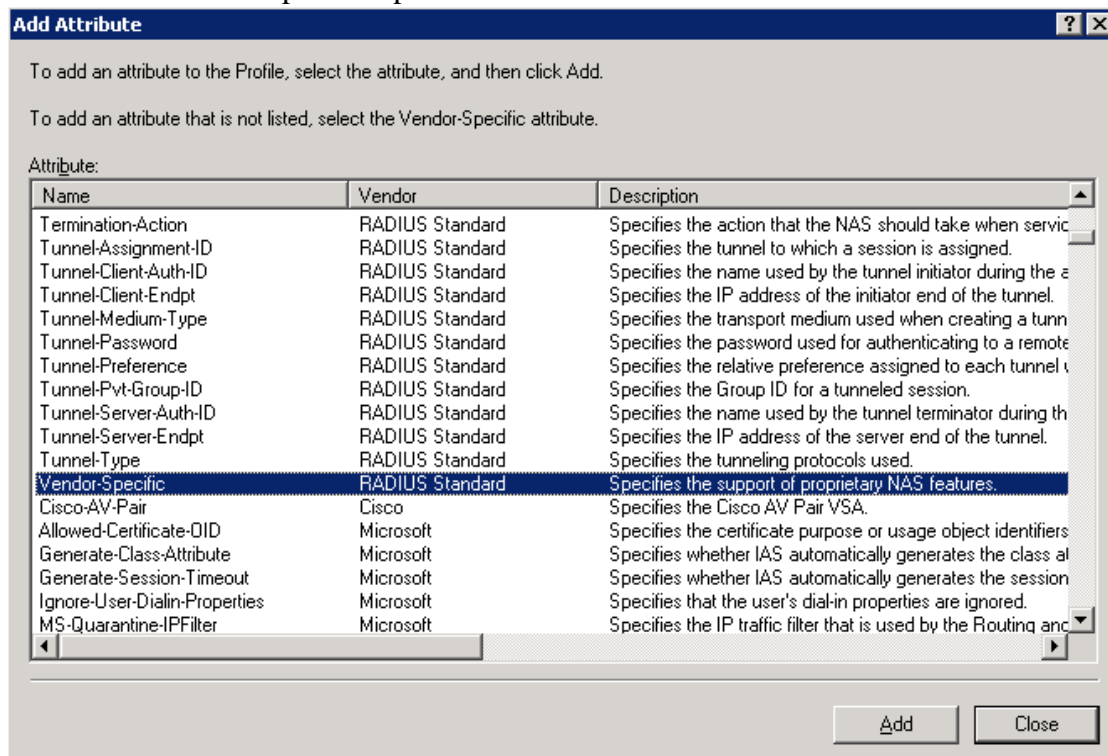
Click on the Authentication tab and select the below authentication method that includes PAP and MSCHAP. Click on the Apply button to save the changes.



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

Multivalued Attribute Information [?] [X]

Attribute name:
Vendor-Specific

Attribute number:
26

Attribute format:
OctetString

Attribute values:

Vendor	Value

Move Up
Move Down
Add
Remove
Edit

OK Cancel

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

Vendor-Specific Attribute Information [?] [X]

Attribute name:
Vendor-Specific

Specify network access server vendor.

☐ Select from list: RADIUS Standard

☒ Enter Vendor Code: 14823

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

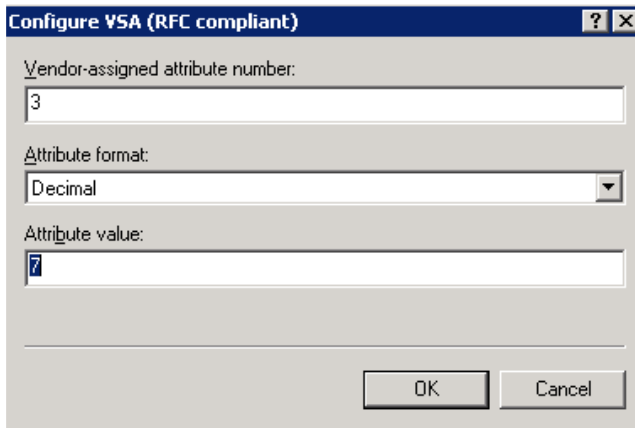
☒ Yes. It conforms.

☐ No. It does not conform.

Configure Attribute...

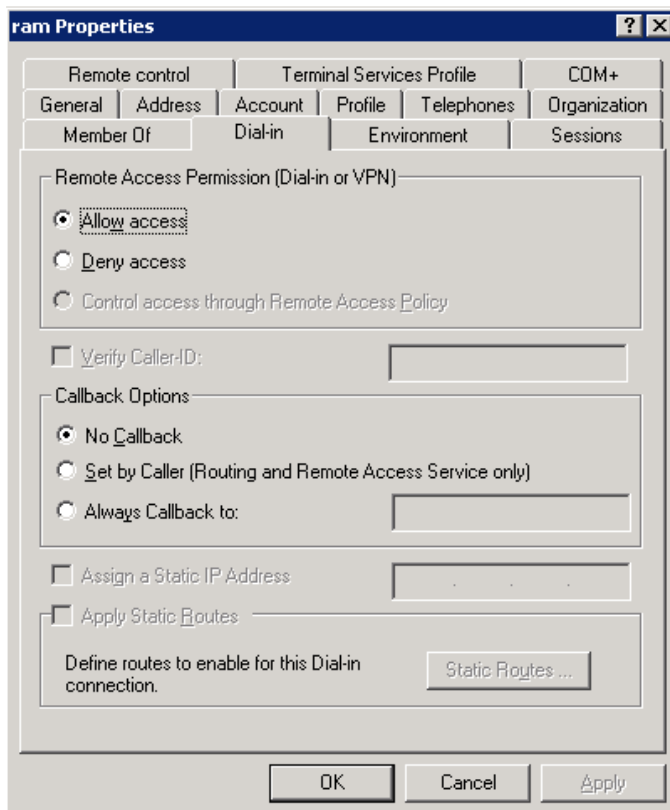
OK Cancel

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



The image shows a Windows dialog box titled "Configure VSA (RFC compliant)". It has three input fields: "Vendor-assigned attribute number:" with the value "3", "Attribute format:" with a dropdown menu set to "Decimal", and "Attribute value:" with the value "7". At the bottom right, there are "OK" and "Cancel" buttons.

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 image shows the "User Properties" dialog box for a user in Windows Active Directory, with the "Dial-in" tab selected. The "Remote Access Permission (Dial-in or VPN)" section has three radio buttons: "Allow access" (selected), "Deny access", and "Control access through Remote Access Policy". Below this is a checkbox for "Verify Caller ID:" which is unchecked. The "Callback Options" section has three radio buttons: "No Callback" (selected), "Set by Caller (Routing and Remote Access Service only)", and "Always Callback to:" with an empty text field. Below this is a checkbox for "Assign a Static IP Address" which is unchecked. The "Apply Static Routes" section has a checkbox which is unchecked, and a button labeled "Static Routes ...". At the bottom, there are "OK", "Cancel", and "Apply" buttons.

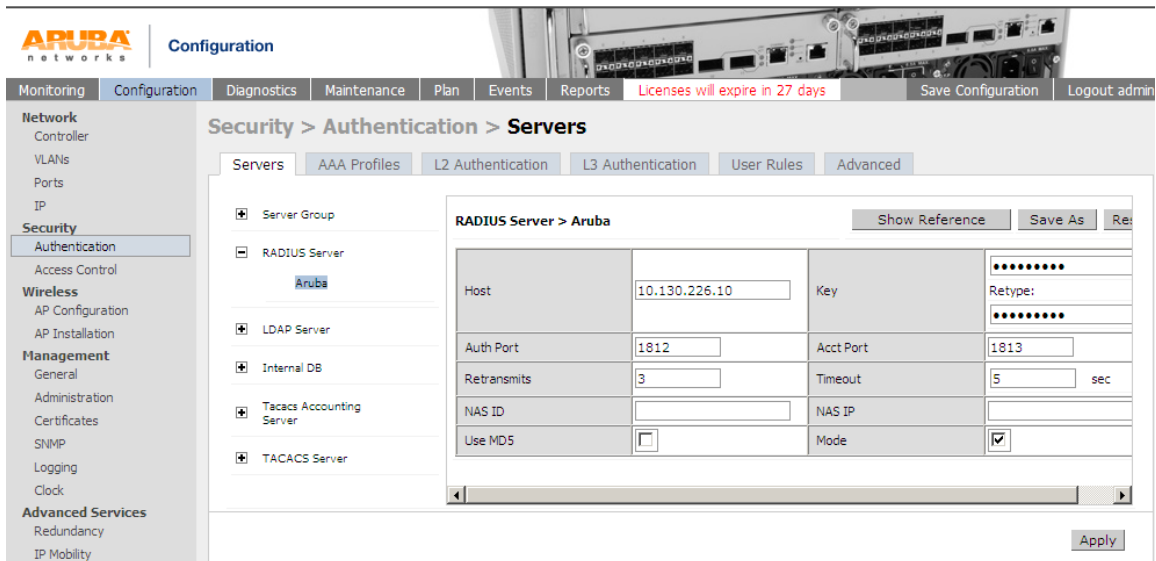
The setting we have to configure on the Aruba controller or Switch.

FROM WEBUI:

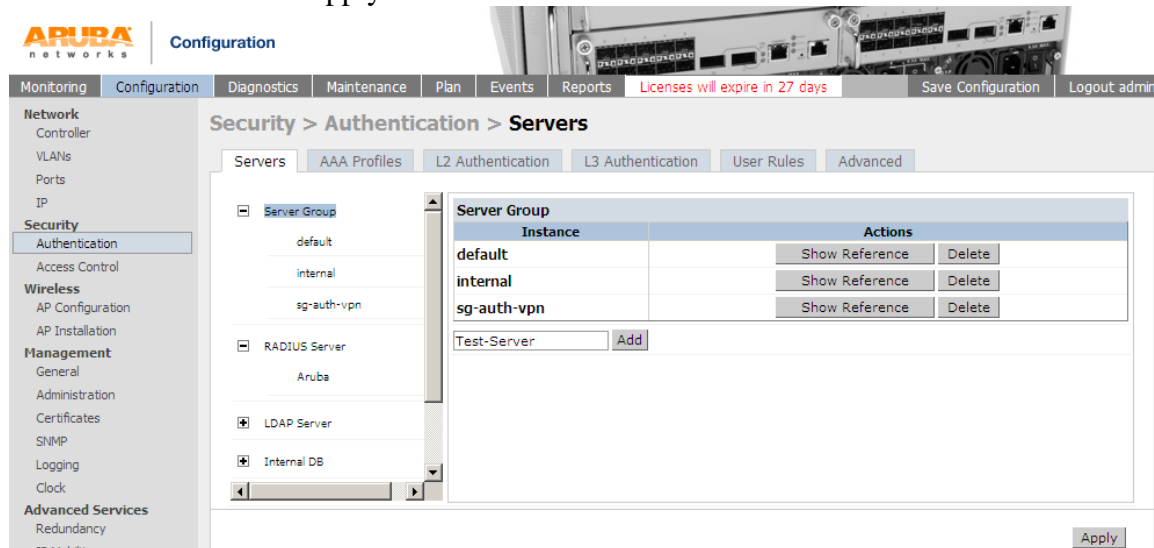
Please navigate to Configuration tab-> Under Security click on Authentication -> Select the Servers tab -> Click on RADIUS Server -> Specify any name e.g. Aruba -> add -> Apply



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

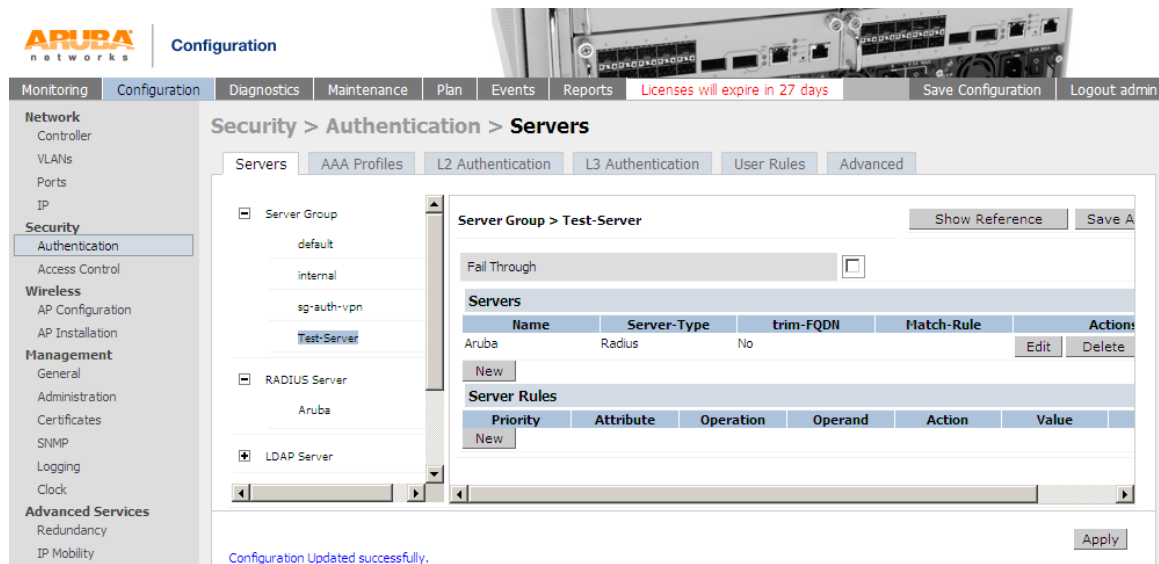


Click on the Server Group under the same window and create a new server group e.g. Test-Server -> Add -> Apply



The screenshot shows the Aruba Configuration interface. The left sidebar lists various configuration categories, with 'Security' expanded and 'Authentication' selected. The main panel is titled 'Security > Authentication > Servers'. It features a 'Server Group' list on the left with options: 'default', 'internal', 'sg-auth-vpn', 'RADIUS Server', 'Aruba', 'LDAP Server', and 'Internal DB'. The 'Test-Server' group is highlighted. On the right, a table shows the configuration for the selected group, with columns for 'Instance' and 'Actions'. The 'Test-Server' instance is listed with 'Show Reference' and 'Delete' buttons. An 'Add' button is visible at the bottom right of the configuration area.

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



The screenshot shows the Aruba Configuration interface. The left sidebar lists various configuration categories, with 'Security' expanded and 'Authentication' selected. The main panel is titled 'Security > Authentication > Servers'. It features a 'Server Group' list on the left with options: 'default', 'internal', 'sg-auth-vpn', 'Test-Server', 'RADIUS Server', 'Aruba', 'LDAP Server', and 'Internal DB'. The 'Test-Server' group is highlighted. On the right, a table shows the configuration for the selected group, with columns for 'Name', 'Server-Type', 'trim-FQDN', 'Match-Rule', and 'Actions'. The 'Test-Server' instance is listed with 'Show Reference' and 'Save A' buttons. A 'New' button is visible at the bottom right of the configuration area. Below the table, a 'Server Rules' section is visible with columns for 'Priority', 'Attribute', 'Operation', 'Operand', 'Action', and 'Value'. A 'New' button is also present in this section. At the bottom, a message states 'Configuration Updated successfully.'

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

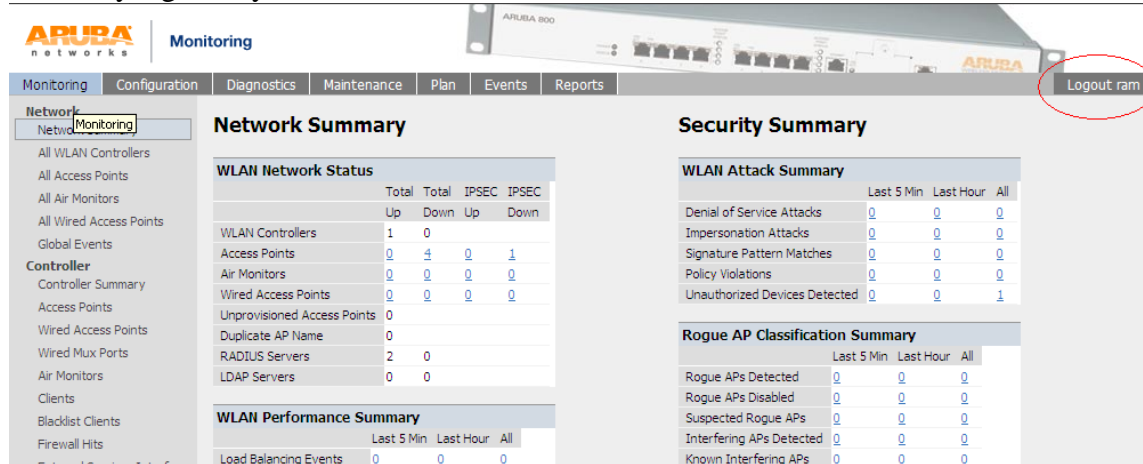
If you will see the Authentication successful means communication happens between Aruba controller and Radius server.

The screenshot shows the Aruba Networks Diagnostics page. The left sidebar contains a menu with categories: Network (Ping, Traceroute, AAA Test Server, Debug Config), General (Technical Support, SSH Terminal), and Access Point (Received Configuration, Software Status, Debug Log, Technical Support, Detailed Statistics, Web Diagnostics). The main content area is titled 'Network > AAA Test Server'. It features a form with the following fields: 'Server Name' (Aruba (IP Address: 10.130.226.10 - Radius)), 'Authentication method' (radio buttons for MSCHAPv2 and PAP, with MSCHAPv2 selected), 'Username' (ram), and 'Password' (masked with dots). A 'Begin Test' button is located below the password field. Below the form, the text 'Authentication successful' is displayed. At the top of the page, there is a navigation bar with tabs: Monitoring, Configuration, Diagnostics (active), Maintenance, Plan, Events, Reports, and a status bar indicating 'Licenses will expire in 27 days' and a 'Logout admin' link.

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

The screenshot shows the Aruba Networks Configuration page. The left sidebar contains a menu with categories: Network (Controller, VLANs, Ports, IP), Security (Authentication, Access Control), Wireless (AP Configuration, AP Installation), Management (General, Administration (active), Certificates, SNMP, Logging, Clock), and Advanced Services (Redundancy, IP Mobility, Stateful Firewall). The main content area is titled 'Management > Administration'. It contains several sections: 'Management Users' with a table showing an 'admin' user with role 'root' and 'Edit'/'Delete' actions; 'Management Authentication Servers' with a 'Default Role' dropdown set to 'root' and a 'Mode' checkbox checked; and 'Server Group' with a dropdown menu showing options: default, internal, sg-auth-vpn, Test-Server (highlighted), and --NEW--. Below the dropdown is a 'Fail Through' checkbox. At the bottom, there is a 'Servers' table with columns: Name, Server-Type, trim-FQDN, Match-Rule, and Actions. A 'New' button is next to the table. The top navigation bar is identical to the previous screenshot, with the 'Configuration' tab active.

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) #