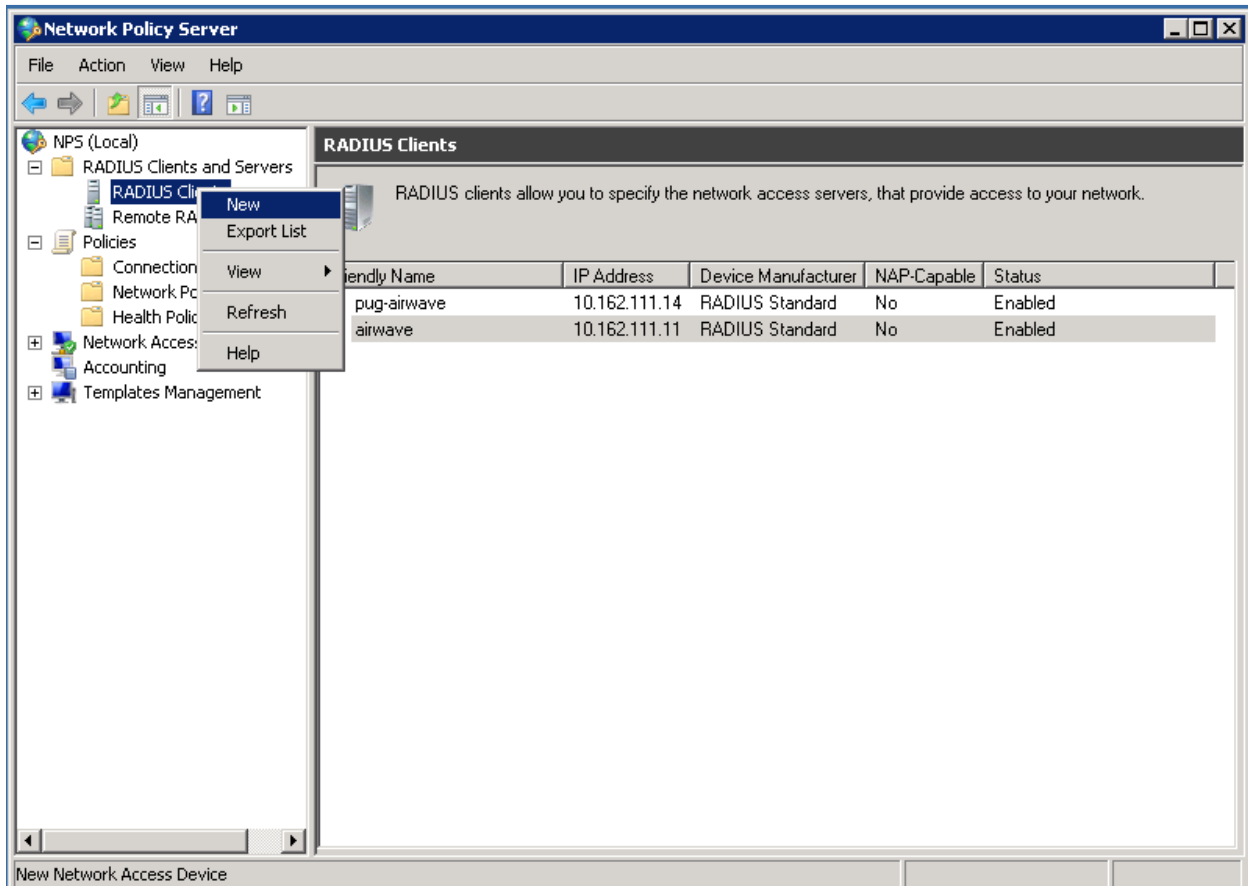


Management Authentication using Windows 2008 as a Radius Server

Given below are the steps on how to configure a Windows 2008 Active Directory to work as a RADIUS server for authenticating AMP users.

- Please navigate to Start → All Programs → Administrative Tools → Network Policy Server.
- Please navigate to RADIUS Clients and Servers → RADIUS Clients.
- Right click on RADIUS Clients and select New.



- Under Settings, please enable the option Enable this RADIUS client.
- Type in a friendly name, for example, you may give the FQDN of your AMP server.
- Enter the IP Address of your AMP server under Address.
- Set None for Select an existing Shared Secrets template.
- Select Manual and create a Shared secret.

New RADIUS Client

Settings | **Advanced**

Enable this RADIUS client

Select an existing template:

Name and Address

Friendly name:
happy.corp.airwave.com

Address (IP or DNS):
happy.corp.airwave.com

Shared Secret

Select an existing Shared Secrets template:
None

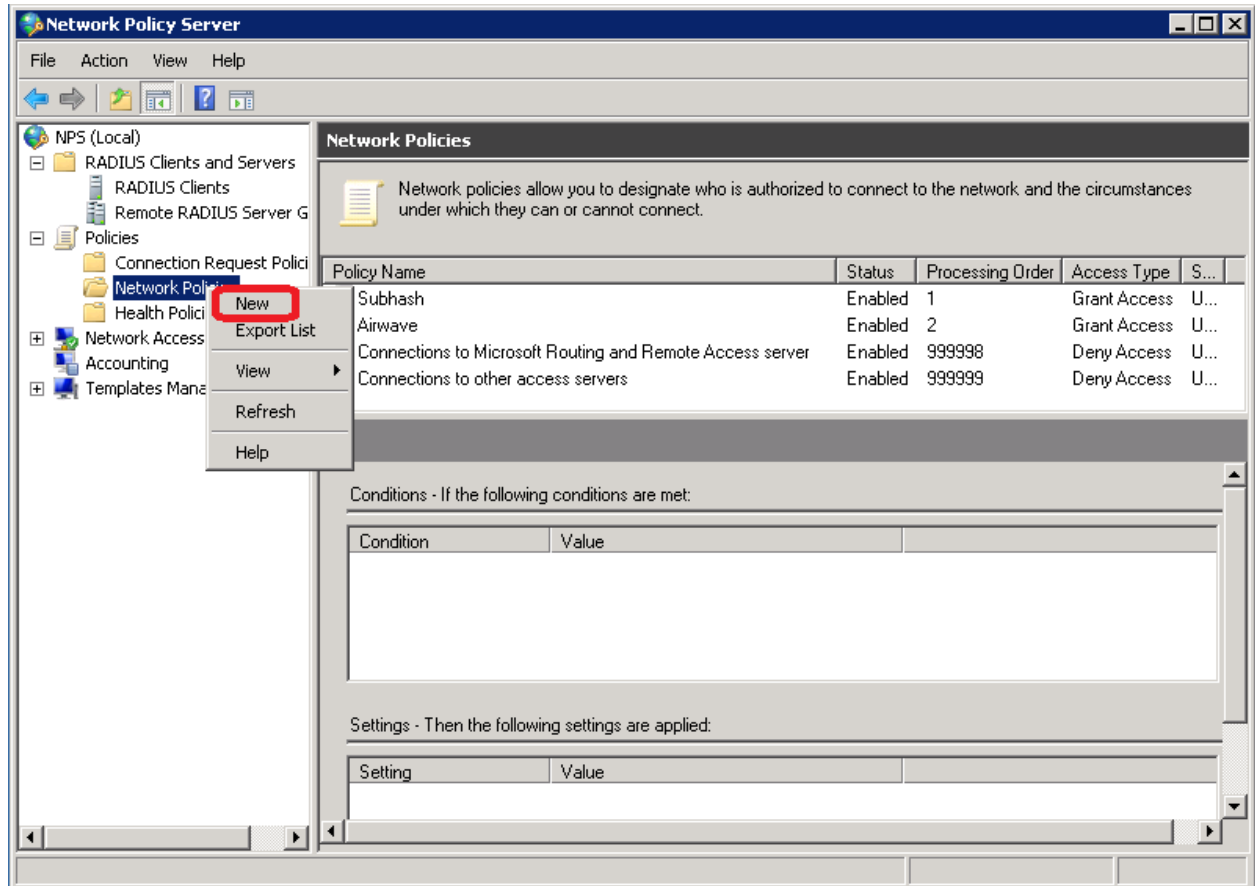
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual Generate

Shared secret:
●●●●●●●


Confirm shared secret:
●●●●●●●

- Please navigate to Policies → Network Policies.
- Right click on Network Policies and select New.



- Enter a Policy Name.
- Select the option Type of network access server and set it to Unspecified and then click on Next.

New Network Policy [X]

 **Specify Network Policy Name and Connection Type**
You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:


Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:

Vendor specific:

- Click on Add to create a condition.

New Network Policy [X]

 **Specify Conditions**

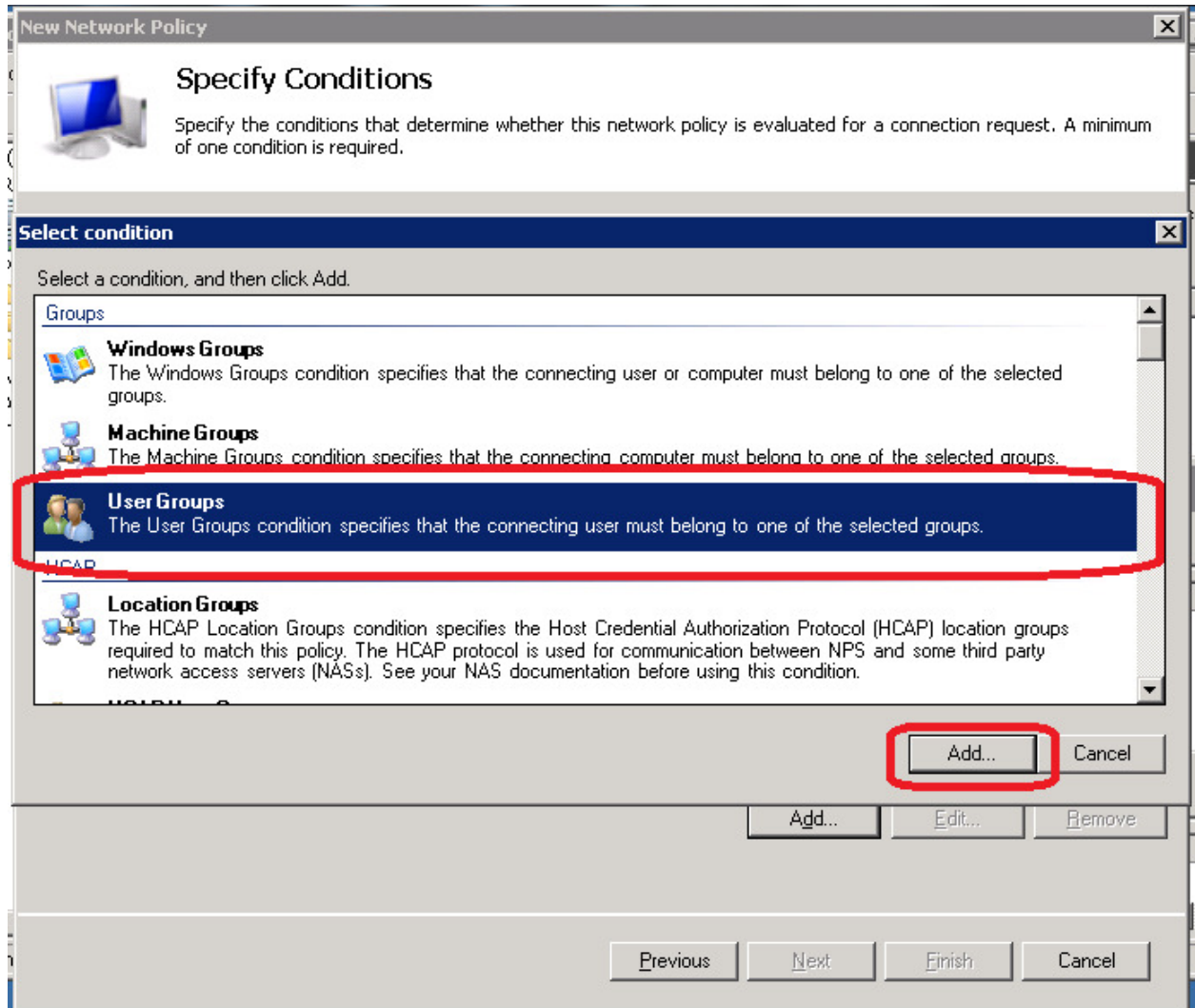
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

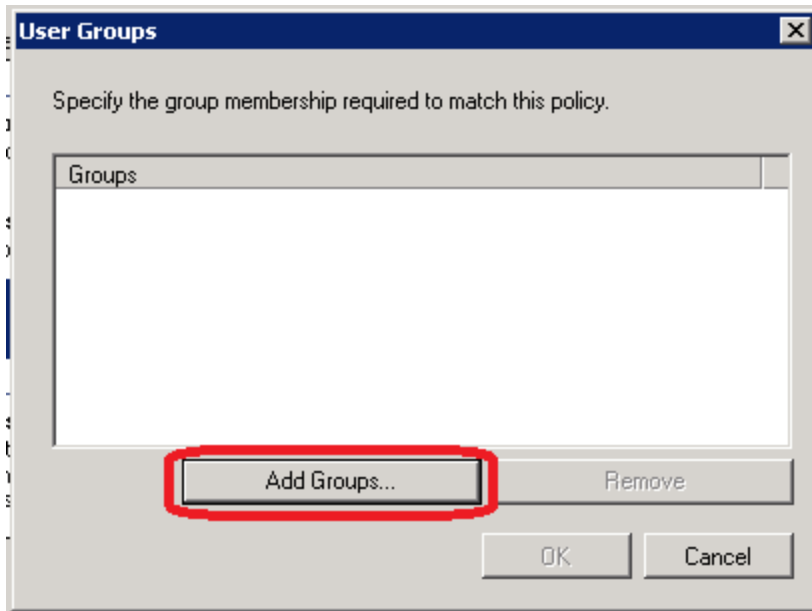
Condition	Value
-----------	-------

Condition description:
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.

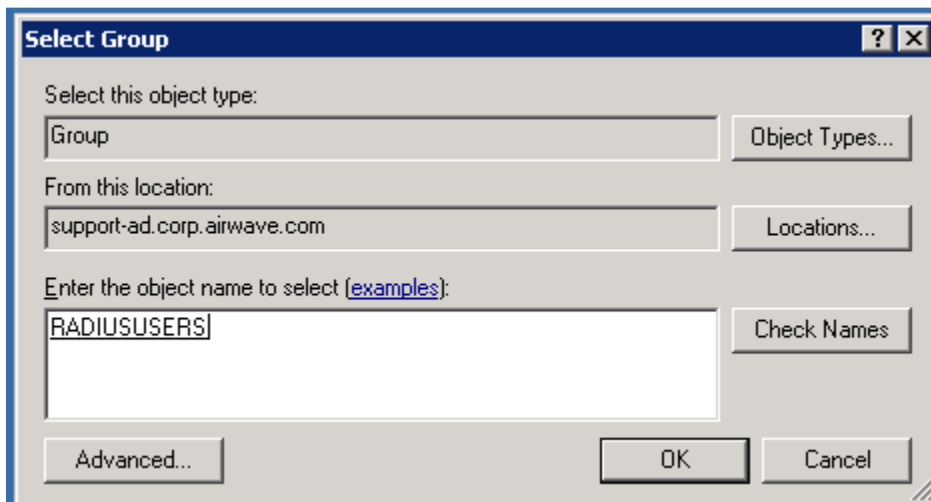
- Select a UserGroup and click on Add.



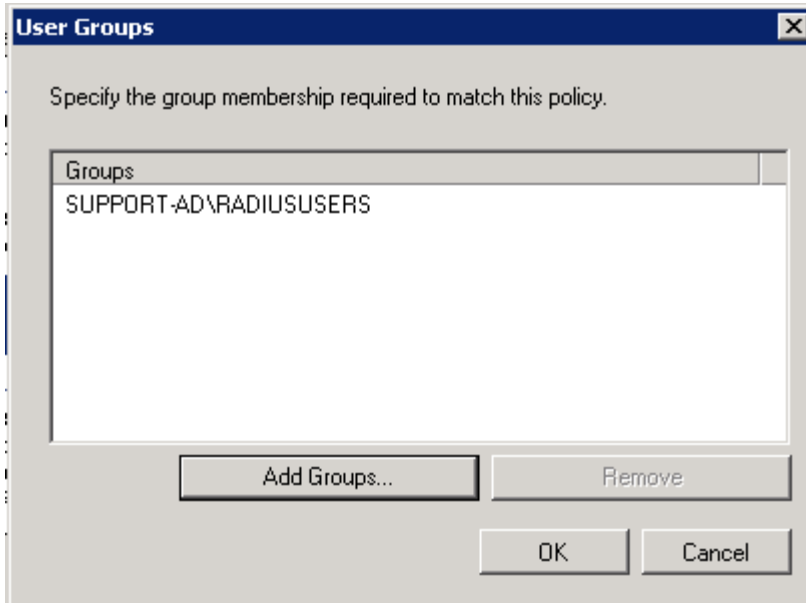
- Please click on Add Groups.



- Enter the desired name of User Group and then click on OK.



- Here the entered User Group would be displayed, now click on OK.



- Click on Add, again to create one more condition.

New Network Policy [X]

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

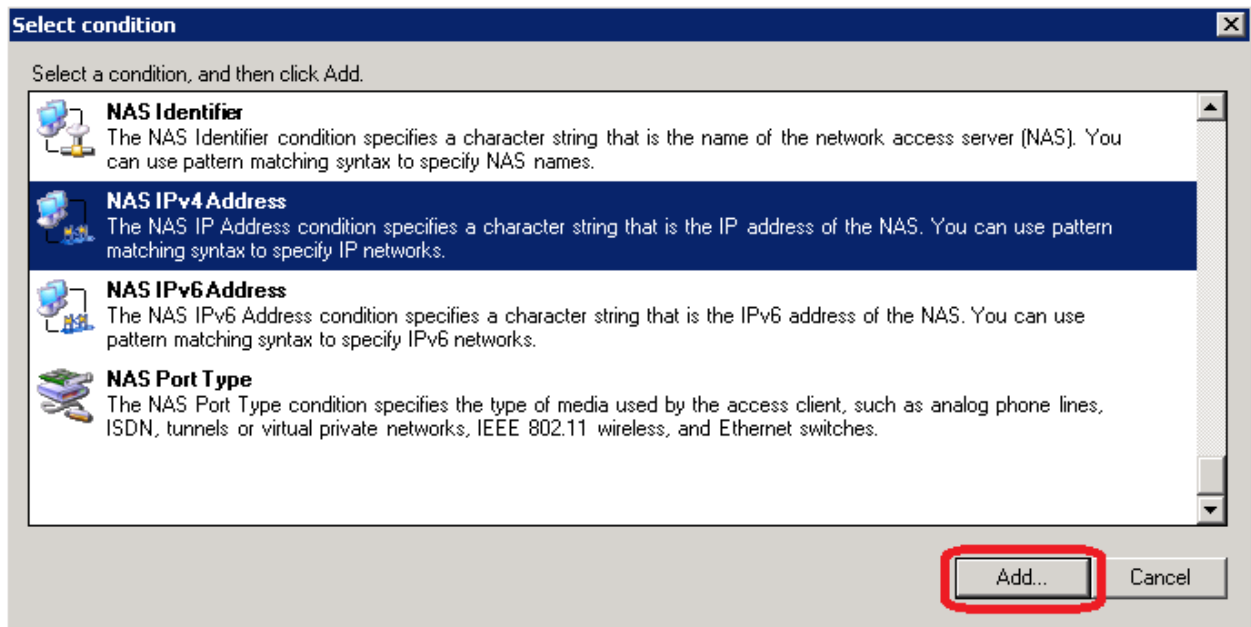
Condition	Value
User Groups	SUPPORT-AD\RADIUSUSERS

Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

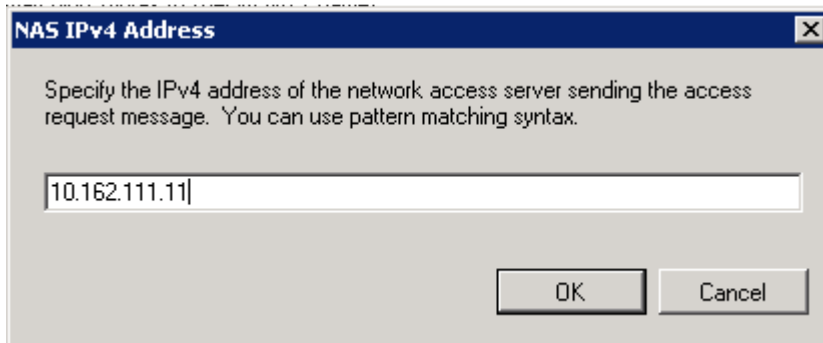
Add... Edit... Remove

Previous Next Finish Cancel

- Select NAS IPv4 Address and then click on Add.




- Enter the IPv4 Address of your AMP server and click on OK.





- Please click on Next on the Conditions screen.

New Network Policy [X]

 **Specify Conditions**

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
 User Groups	SUPPORT-AD\RADIUSUSERS
 NAS IPv4 Address	10.162.111.28


Condition description:
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.

Add... Edit... Remove

Previous **Next** Finish Cancel

- Select Access granted and then please click on Next.

New Network Policy [X]

 **Specify Access Permission**

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

Access granted
Grant access if client connection attempts match the conditions of this policy.

Access denied
Deny access if client connection attempts match the conditions of this policy.

Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

- Please select the authentication methods as shown below:

New Network Policy [X]

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:


Less secure authentication methods:

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
 - User can change password after it has expired
- Encrypted authentication (CHAP)
- Unencrypted authentication (PAP, SPAP)
- Allow clients to connect without negotiating an authentication method.
- Perform machine health check only

- You may get a pop-up regarding a Connection Request Policy, please click on NO.
- You may configure constraints (but this can be left with default values) and then please click on Next.






New Network Policy [X]

Configure Constraints

 Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints	
 Idle Timeout	<p>Specify the maximum time in minutes that the server can remain idle before the connection is disconnected</p> <p><input type="checkbox"/> Disconnect after the maximum idle time</p> <p><input type="text" value="1"/></p>
 Session Timeout	
 Called Station ID	
 Day and time restrictions	
 NAS Port Type	

- Under Configure Settings → RADIUS Attributes → Vendor Specific → Add.

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- RADIUS Attributes**
 - Standard
 - Vendor Specific
- Network Access Protection**
 - NAP Enforcement
 - Extended State
- Routing and Remote Access**
 - Multilink and Bandwidth Allocation Protocol (BAP)
 - IP Filters
 - Encryption
 - IP Settings

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
------	--------	-------

Add... Edit... Remove

Previous Next Finish Cancel

- Set the Vendor to Custom from the drop down menu and then select Vendor-Specific and then please click on Add.

Add Vendor Specific Attribute [X]

To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor:
Custom

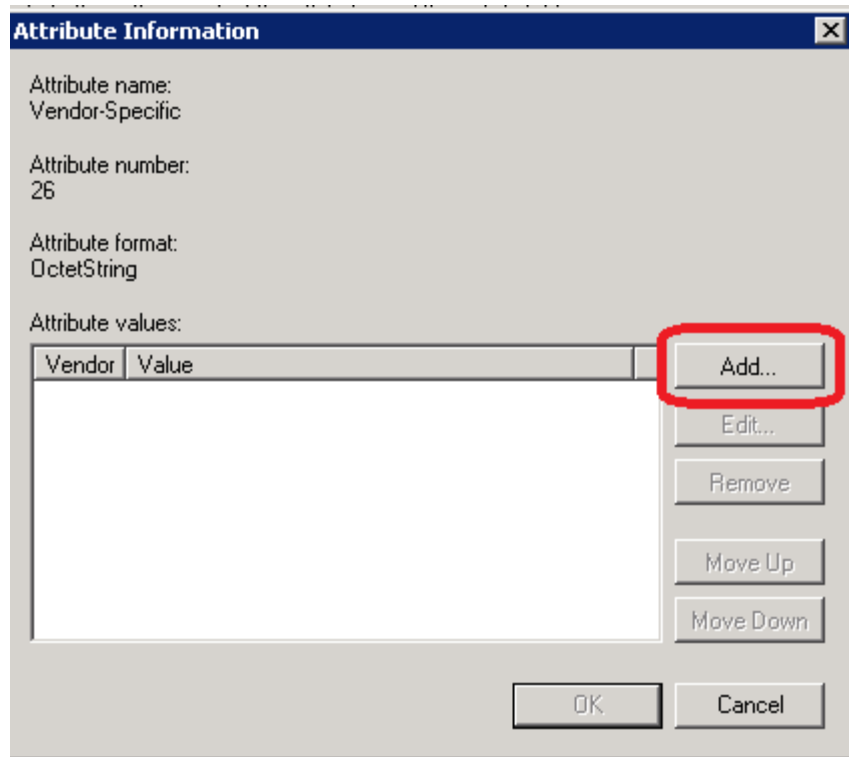
Attributes:

Name	Vendor
Allowed-Certificate-OID	RADIUS Standard
Generate-Class-Attribute	RADIUS Standard
Generate-Session-Timeout	RADIUS Standard
Tunnel-Tag	RADIUS Standard
Vendor-Specific	RADIUS Standard

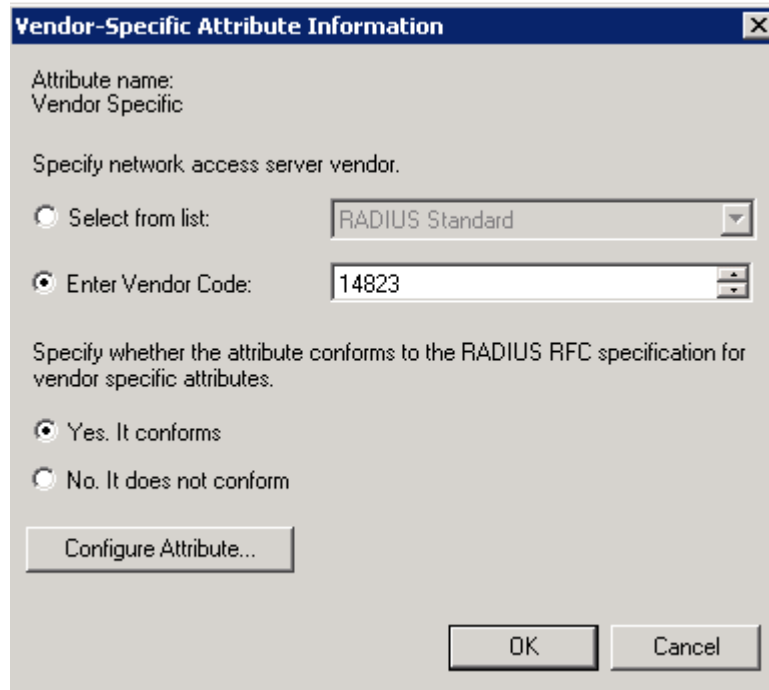
Description:
Specifies the support of proprietary NAS features.

Add... Close

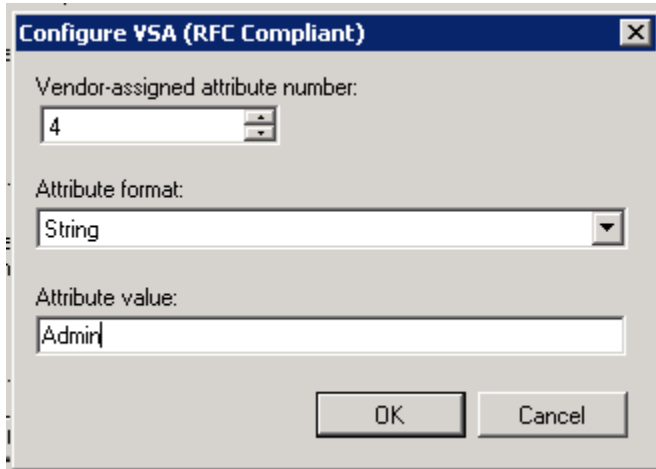
- Under Attribute information, click on Add:



- Enter the Aruba vendor code – 14823.
- Choose Yes. It conforms and please click on Configure Attribute.



- The Vendor assigned attribute number should be set to 4.
- The Attribute format should be set to String.
- The Attribute value should be set to the name of the user-role that would be later created under the AMP Setup → Roles page. Here we have entered Admin user-role.



Configure VSA (RFC Compliant)

Vendor-assigned attribute number:
4

Attribute format:
String

Attribute value:
Admin

OK Cancel

- Please click on Finish.

Policy conditions:

Condition	Value
User Groups	SUPPORT-AD\RADIUSUSERS
NAS IPv4 Address	10.162.111.11

Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 ...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

- Please create a user-role Admin under AMP Setup → Roles page:

Home Groups APs/Devices Users Reports System Device Setup **AMP Setup** RAPIDS VisualRF

General Network Users Roles Guest Users Authentication MDM Server Device Type Setup WLSE ACS NMS RADIUS Accounting PCI Compliance

Add New Role

	Name	Enabled	Type	Access Level	Top Folder	Visible Groups	Allow authorization of APs/Devices	RAPIDS	VisualRF	Allow user to disable timeout
<input type="checkbox"/>	Admin	Yes	AMP Administrator	-	Top	All	Yes	Administrator	Read/Write	Yes
<input type="checkbox"/>	Read-Only Monitoring & Auditing	Yes	AP/Device Manager	Audit (Read Only)	Top	All	Yes	None	Read Only	No

Select All - Unselect All

Delete

- Please navigate to AMP Setup → Authentication page → RADIUS Configuration.
- Set Enable RADIUS Authentication and Authorization to Yes.
- Enter the Primary Server Hostname / IP Address and the Shared Secret.

Home	Groups	APs/Devices	Users	Reports	System	Device Setup	AMP Setup	
General	Network	Users	Roles	Guest Users	Authentication	MDM Server	Device Type Setup	WLS

Login Configuration

Max AMP User Idle Timeout (Greater than or equal to 5 min):

Login message:

TACACS+ Configuration

Enable TACACS+ Authentication and Authorization: Yes No

RADIUS Configuration

Enable RADIUS Authentication and Authorization: Yes No

Primary Server Hostname/IP Address:

Primary Server Port (1-65535):

Primary Server Secret:

Confirm Primary Server Secret:

Secondary Server Hostname/IP Address:

Secondary Server Port (1-65535):

Secondary Server Secret:

Confirm Secondary Server Secret:

- Click on Save.

Now you should be able to authenticate all the users in your User Group on the Windows 2008 server when they login to the AMP.