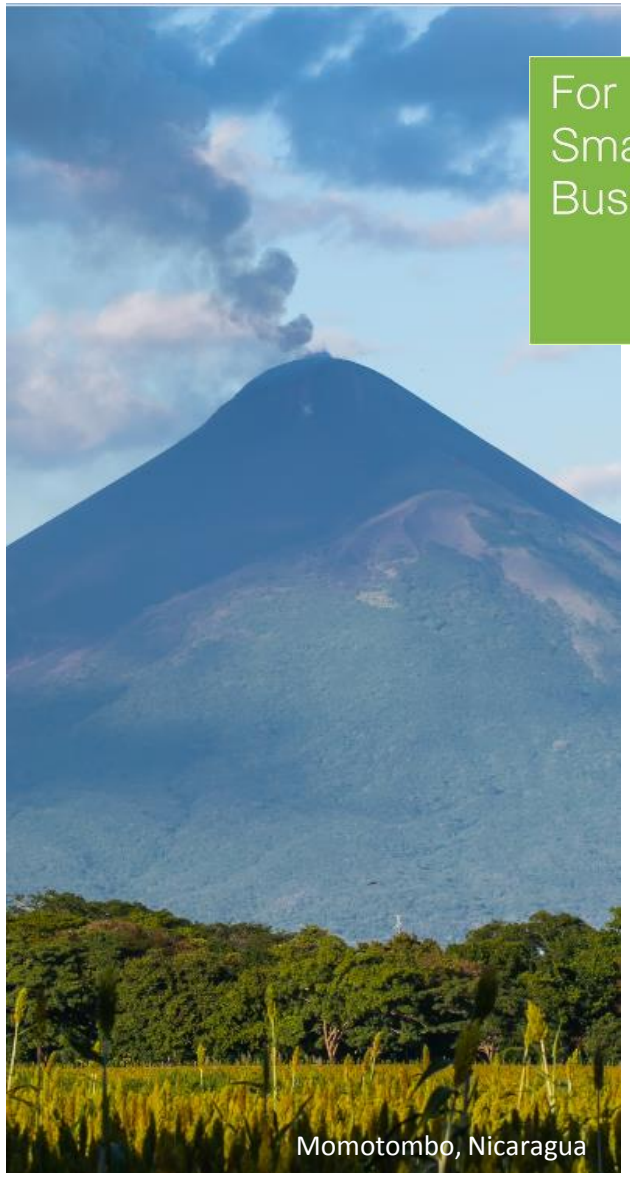
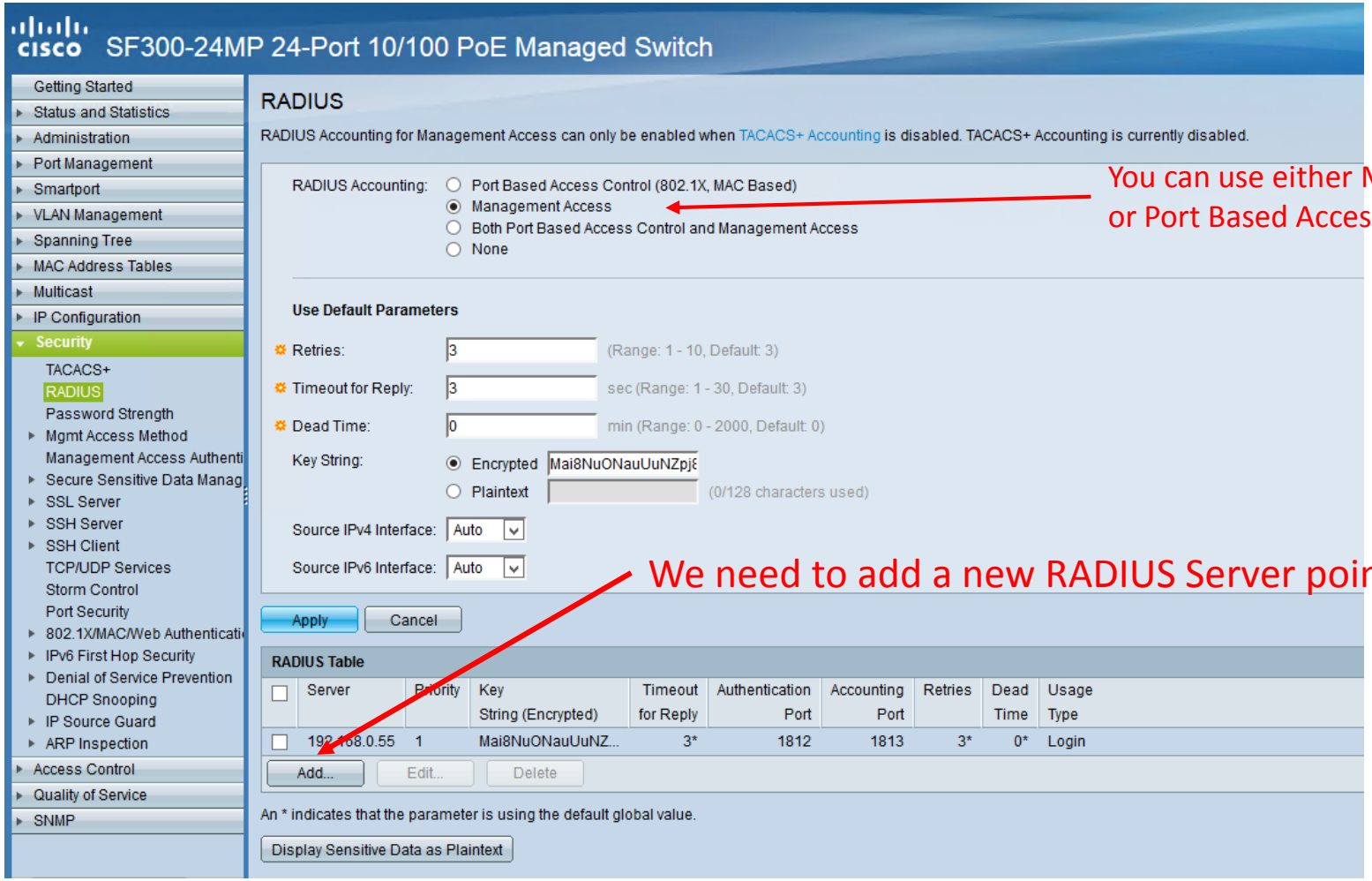


Windows Server NPS (Radius) with SMB Switches

Authentication for GUI, Web and SSH, etc.

1. Configure Switch Security Setting (Radius)

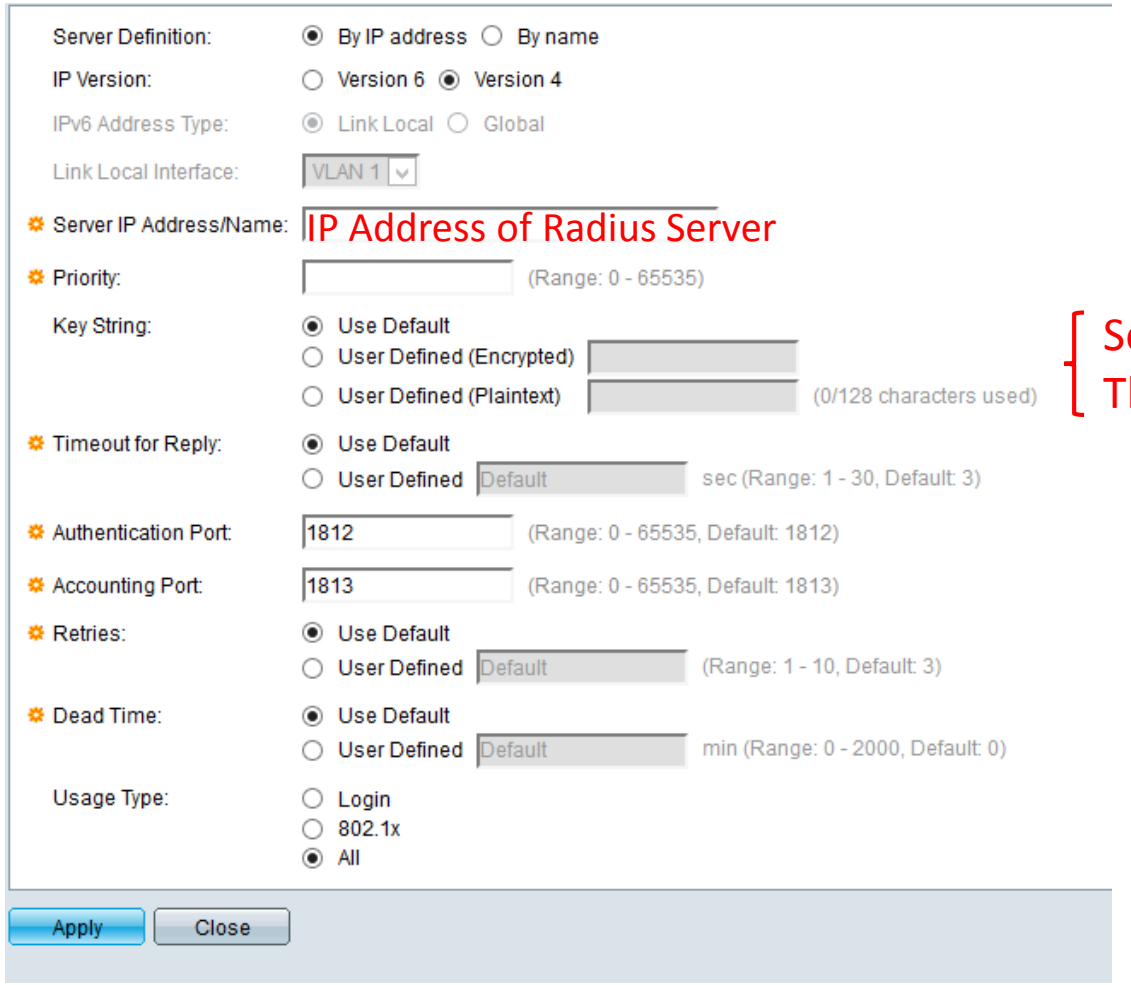


You can use either Management Access or Port Based Access Control

We need to add a new RADIUS Server point of contact

For Small Business

2. Fill all the information required for Radius

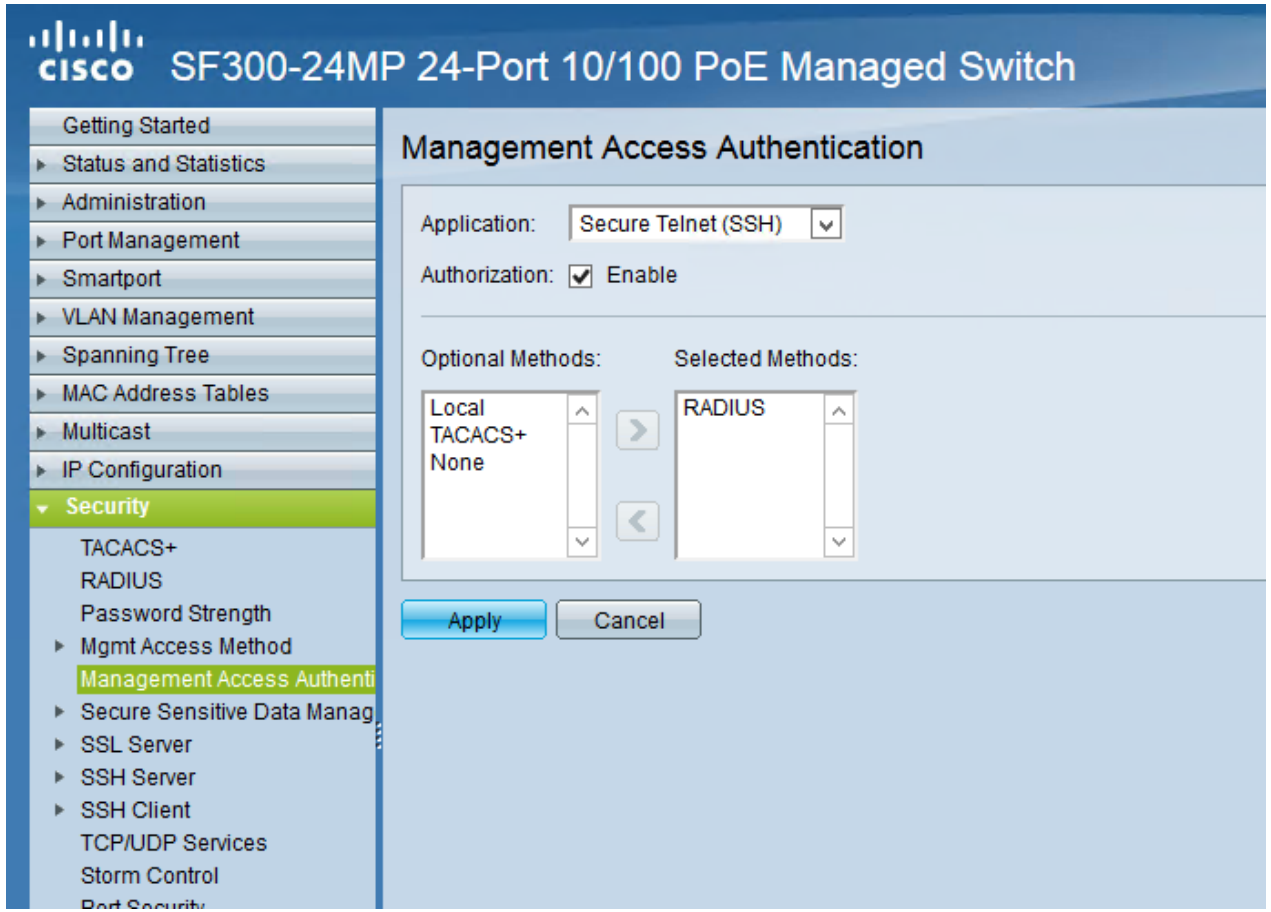


Select Plaintext to enter the PSK
This will be set on Radius Settings

For Small Business

cisco

3. Go to “Management Access Authentication”



On Application, you can select the access method to evaluate with Radius Server such as:

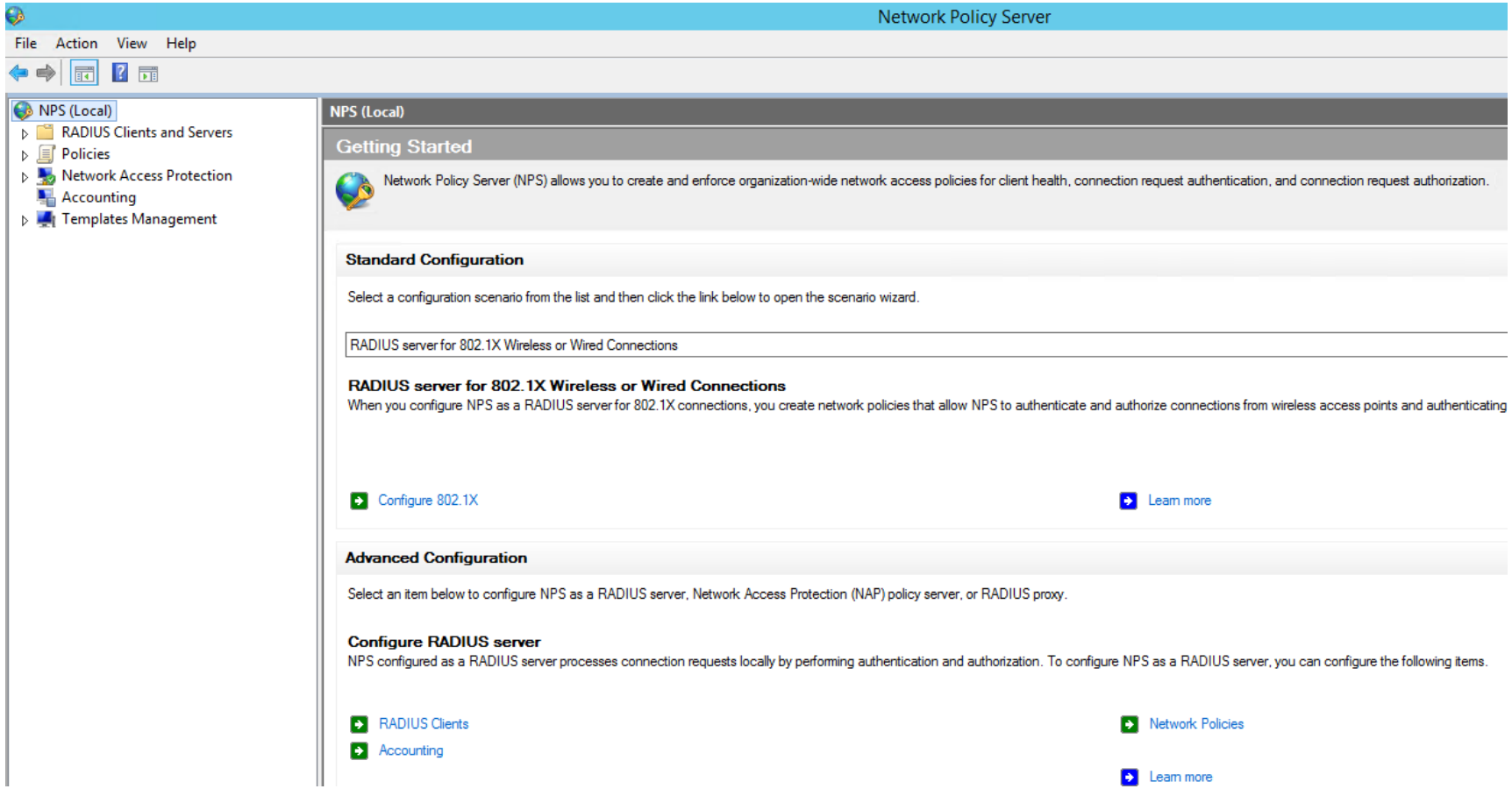
- Console
- Web Access (http, https)
- CLI (telnet, SSH)

To make this works you need to:

1. Enable “Authorization”
2. Delete Local value from Selected Methods list by click on < button.
3. Add RADIUS value from Optional Methods by click on > button.
4. Apply the changes.

For Small Business

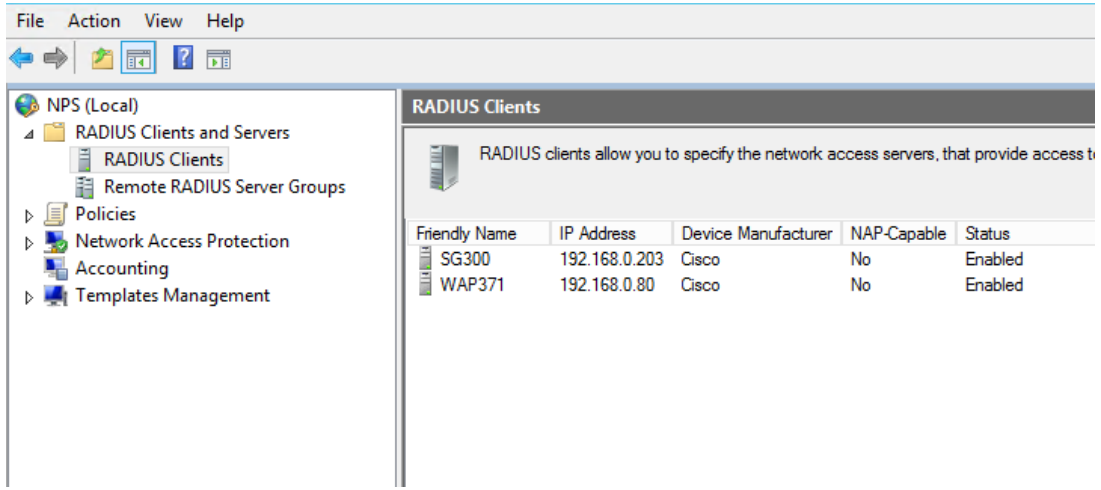
4. Open Windows NPS (Radius Server)

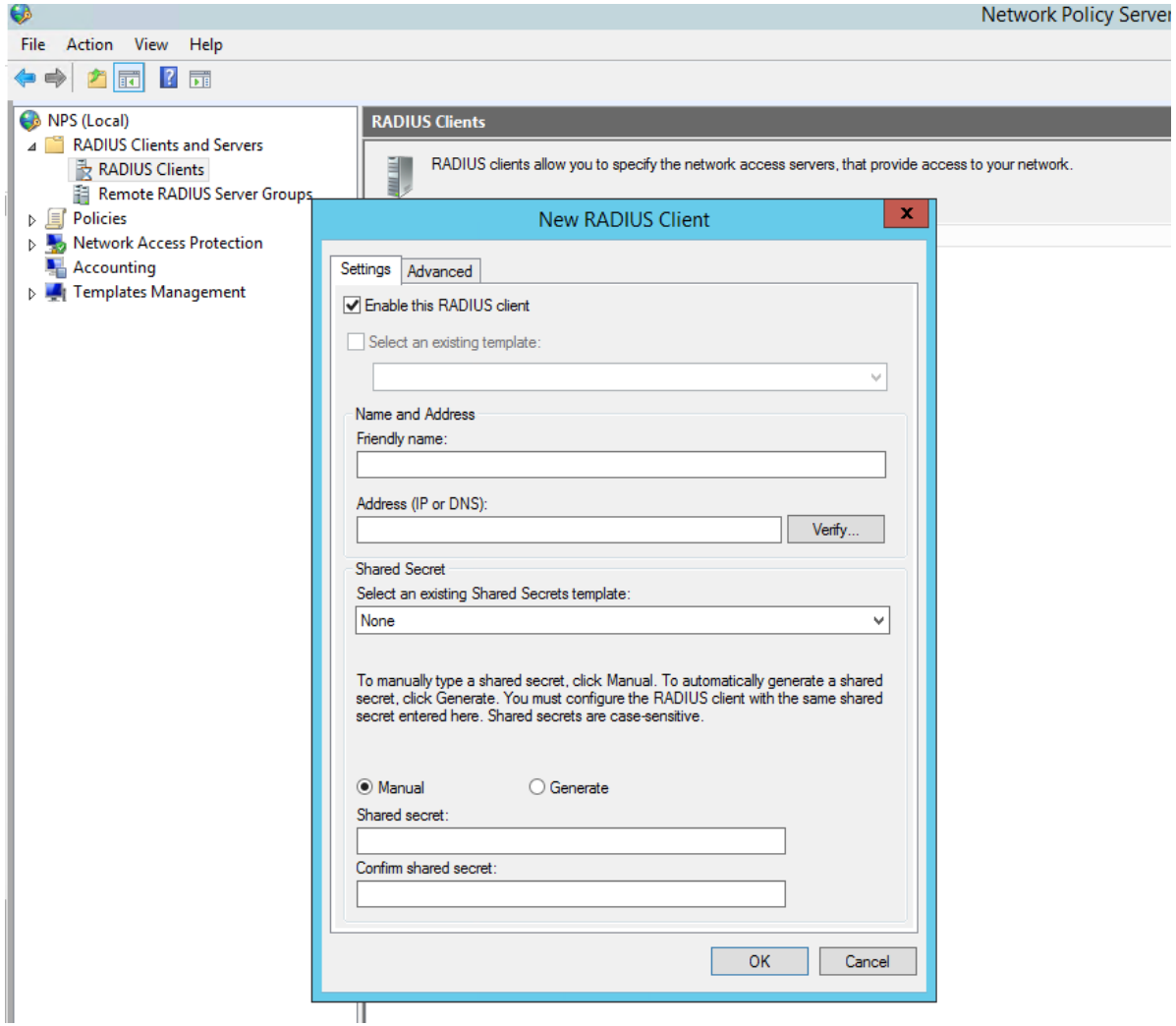


For Small Business

cisco

5. Create a new RADIUS Clients



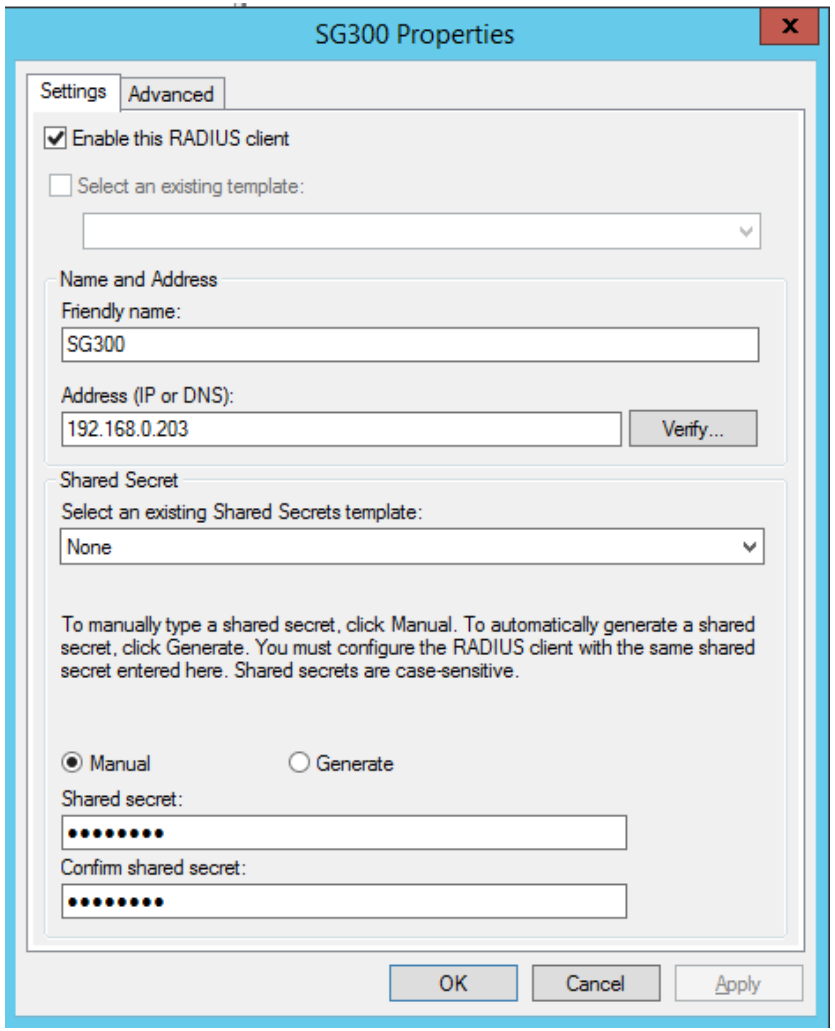


You will need to expand «Radius Clients and Server» option and then right click on RADIUS CLIENTS and select New

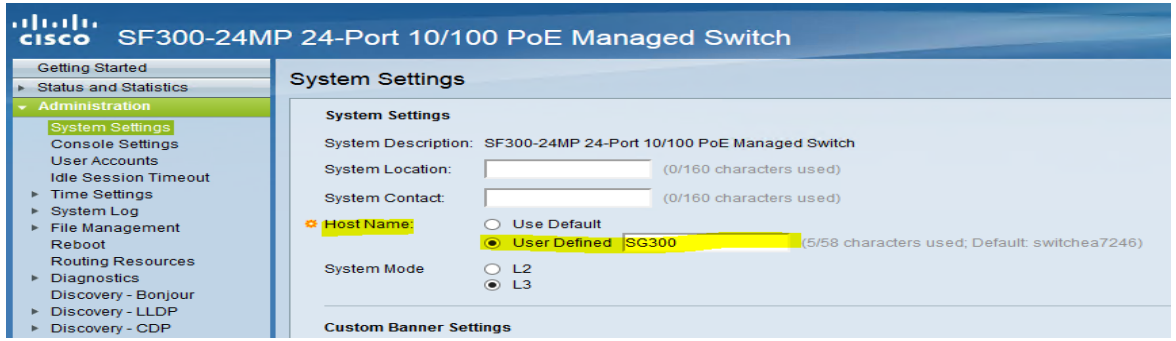
For Small Business

cisco

6. Fill the information for new Radius Client

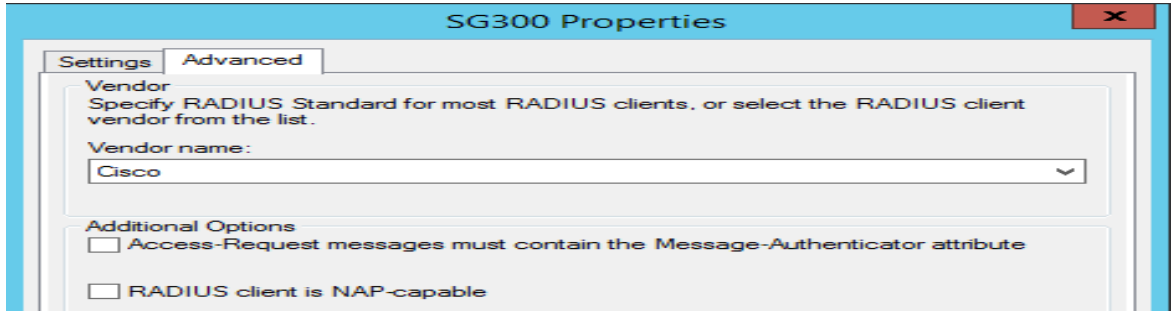


* Friendly Name is referring to Hostname of the Switch



* Address (IP or DNS) is referring to SW IP address
* Shared Secret, this will be the PSK set on the SW.

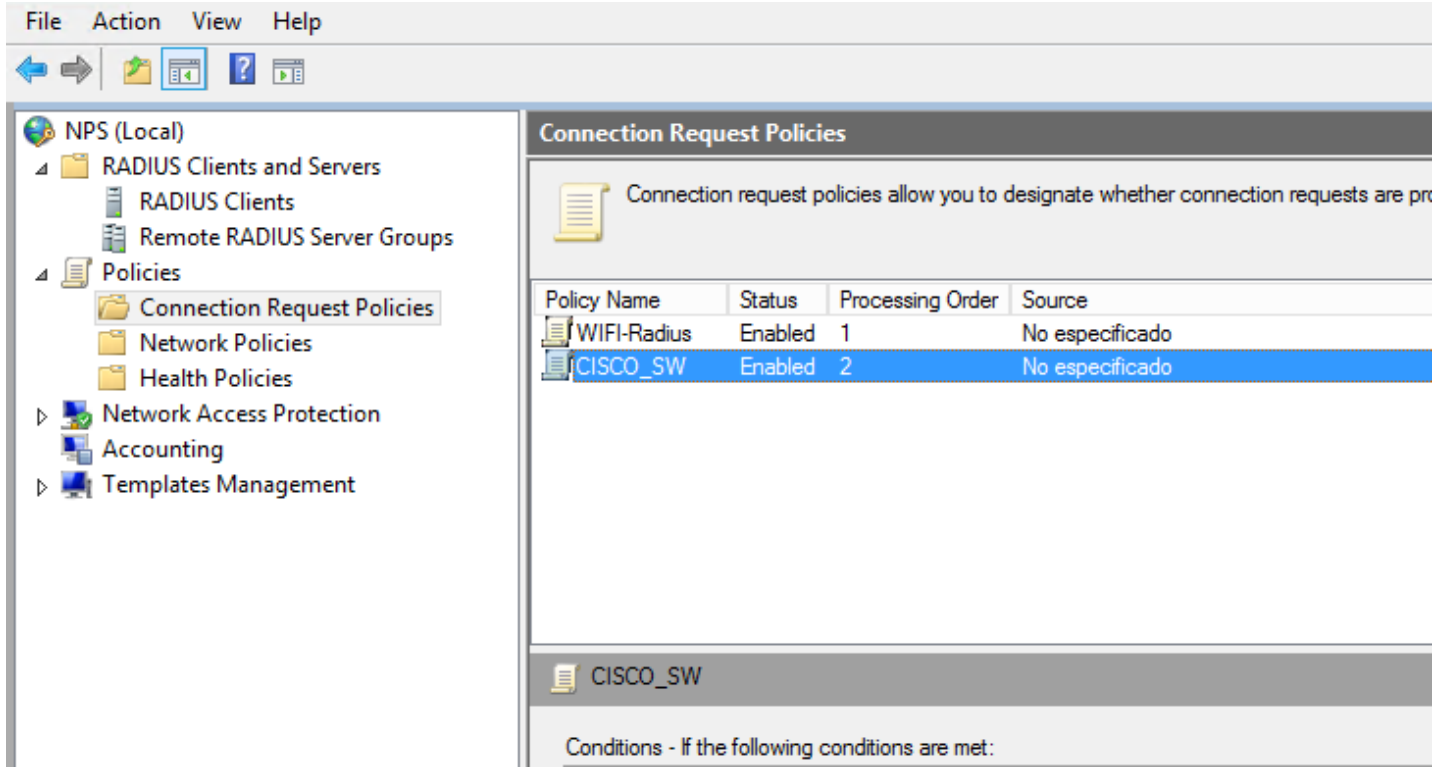
On Advance Tap we need to select Cisco as Vendor Name:



For Small Business

cisco

7. Verify Radius Policies



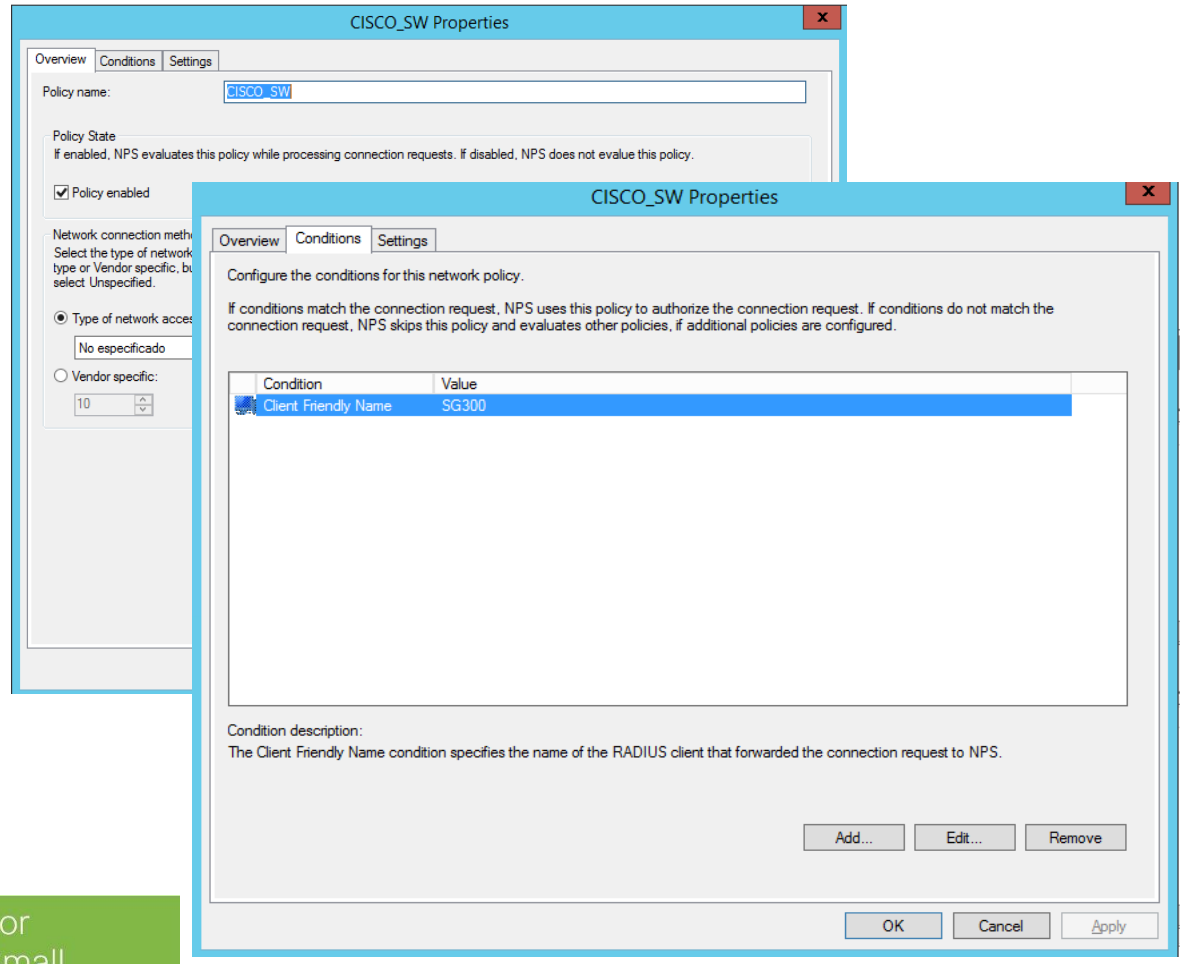
We need to verify two Policies:

1. Connection Request Policies and
2. Network Policies

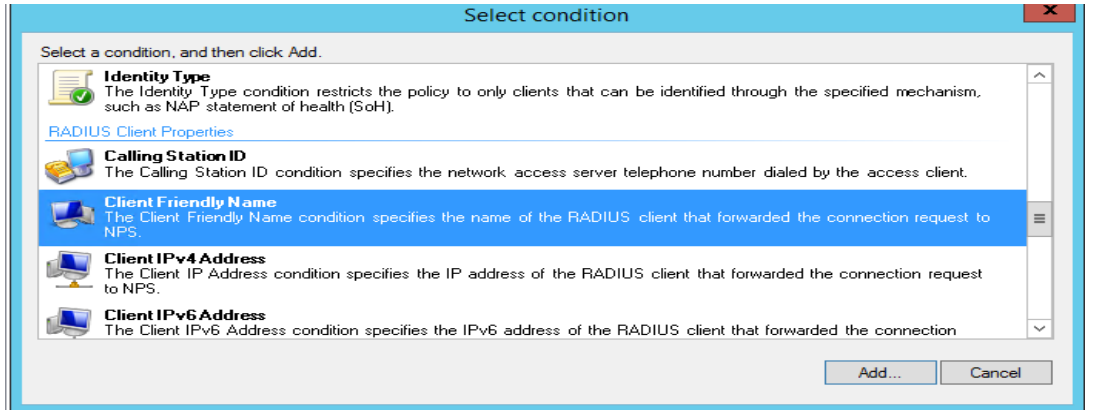
For Small Business

cisco

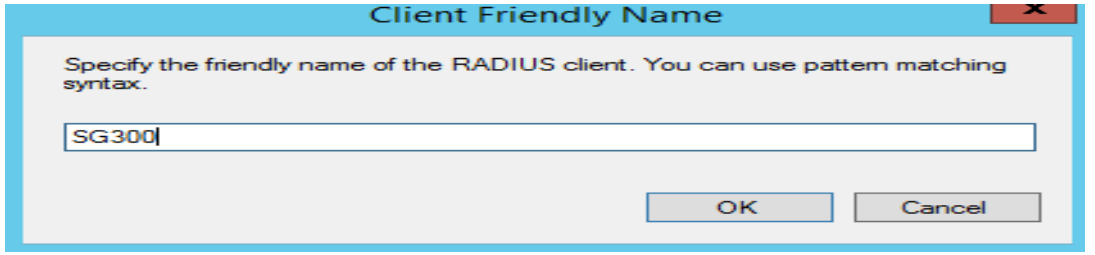
8.A - Create a new Connection Request Policies



On Conditions tab you need to add a new condition row, just click on Add button and look for the option “Client Friendly Name”



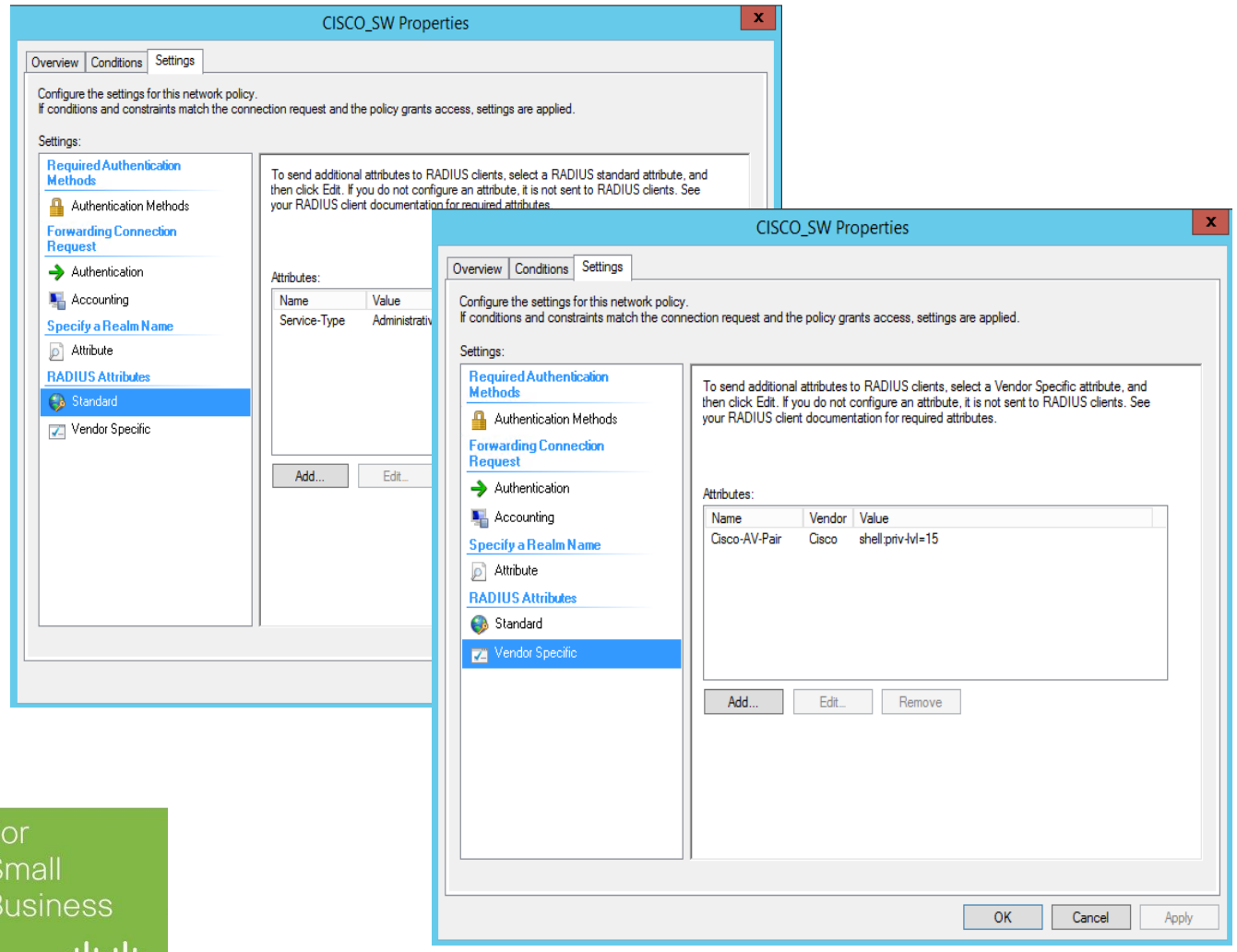
And type the hostname of SW.



For Small Business

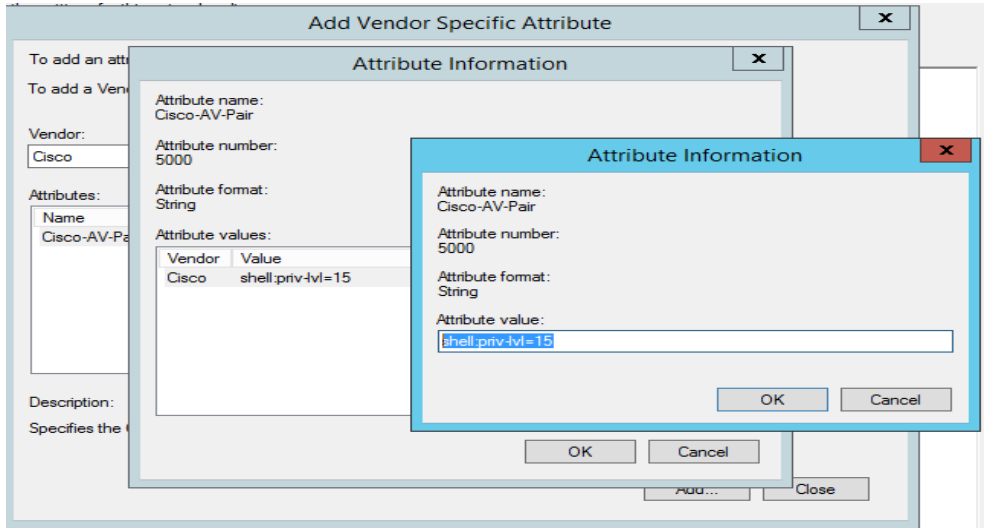
cisco

8.B - Verify the Setting tab before save the policy



We must add the Radius Attributes for:

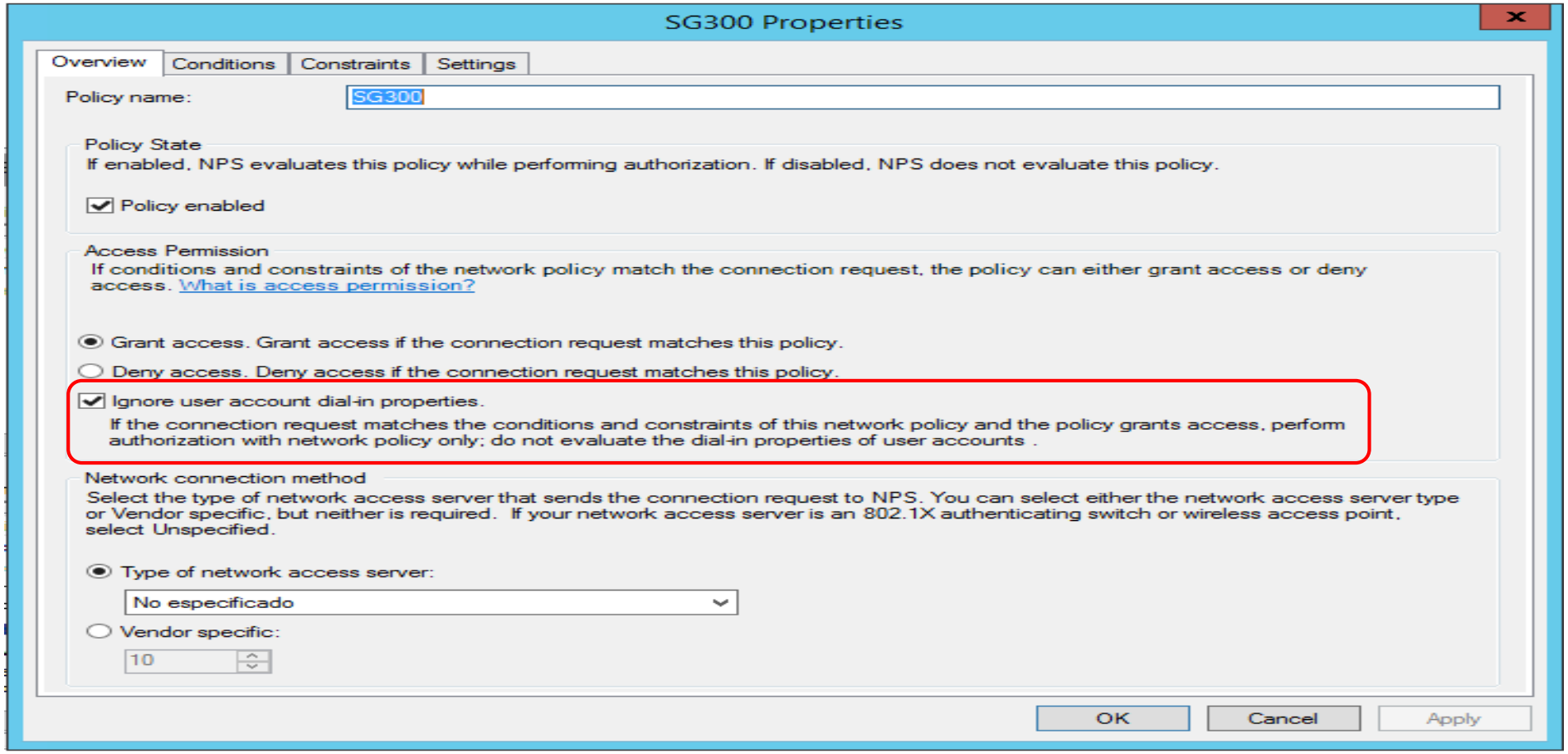
1. Standard
    1. Name: Services-Type
    2. Value: administrative
2. Vendor Specific:
    1. Name: Cisco-AV-Pair
    2. Vendor: Cisco
    3. Value: shell:priv-lvl=15



For Small Business

cisco

9. Network Policies - Overview

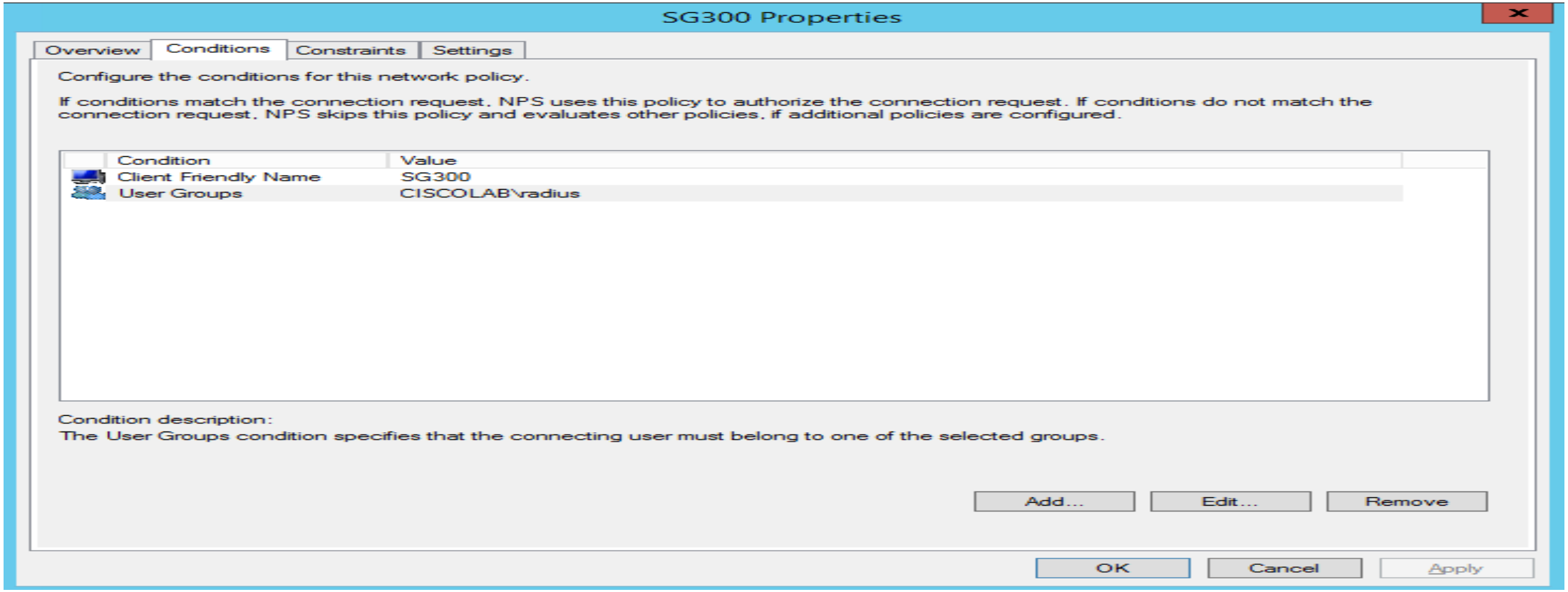


We need to enable the “Ignore user account dial-in properties” option

For Small Business

cisco

9. Network Policies - Conditions

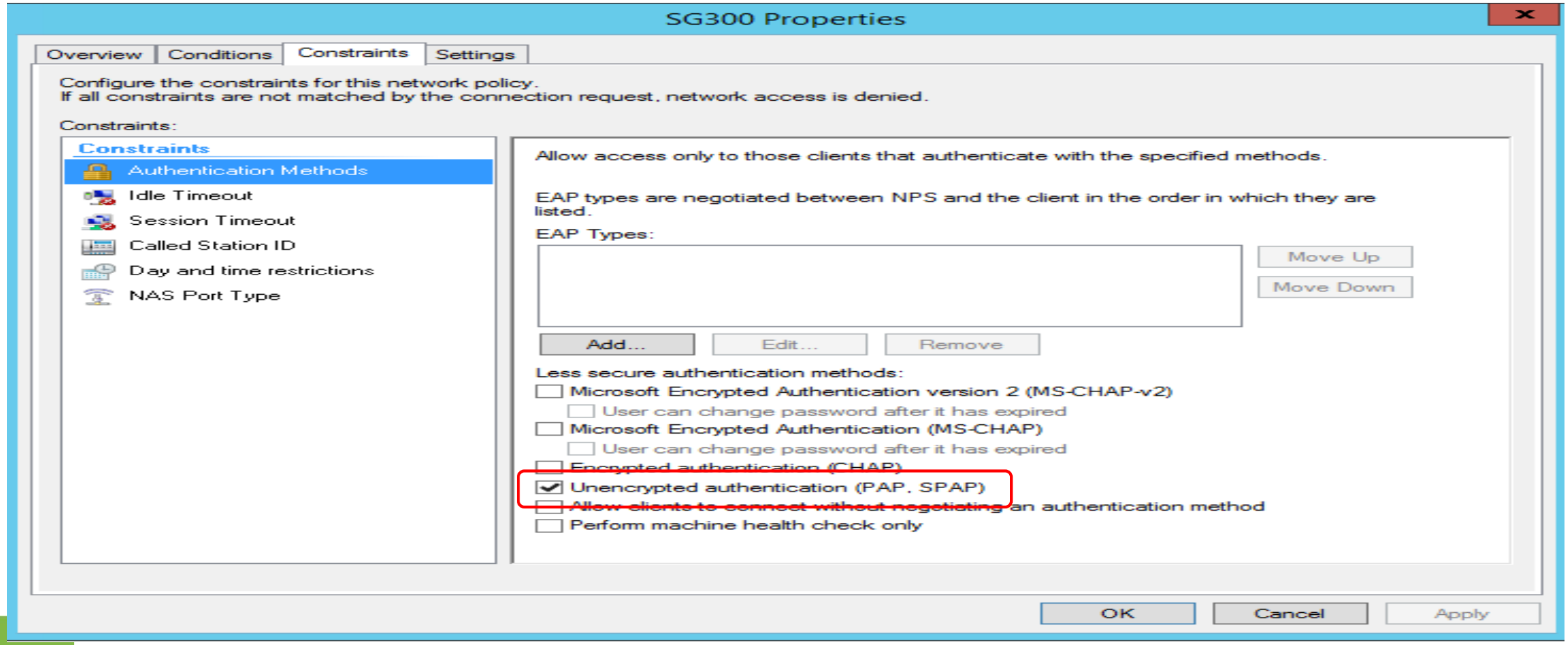


- We need to add:
  - Client friendly name
  - User group to use.

For Small Business

cisco

9. Network Policies – Constraints

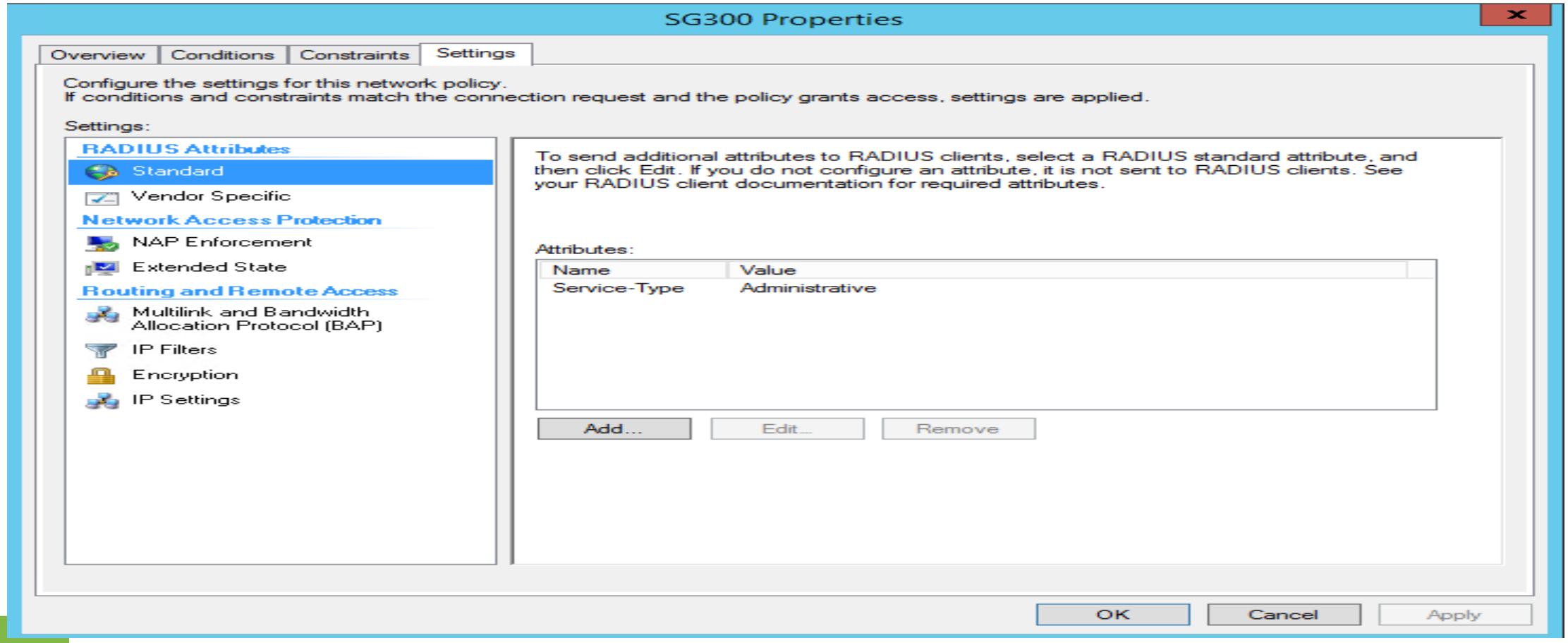


- Uncheck everything then select Unencrypted authentication (PAP, SPAP)

For Small Business

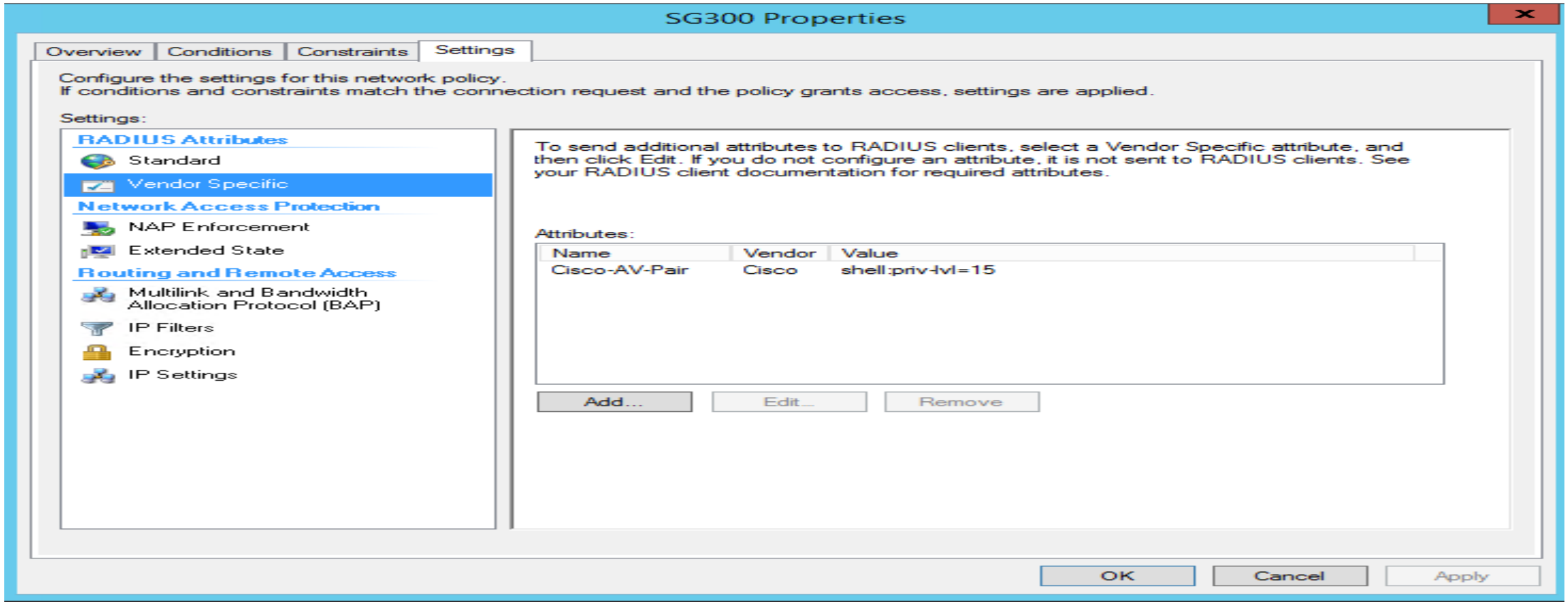
cisco

9. Network Policies – Settings



•Select and remove the Framed-Protocol and set Service-Type attributes

9. Network Policies – Settings * Vendor

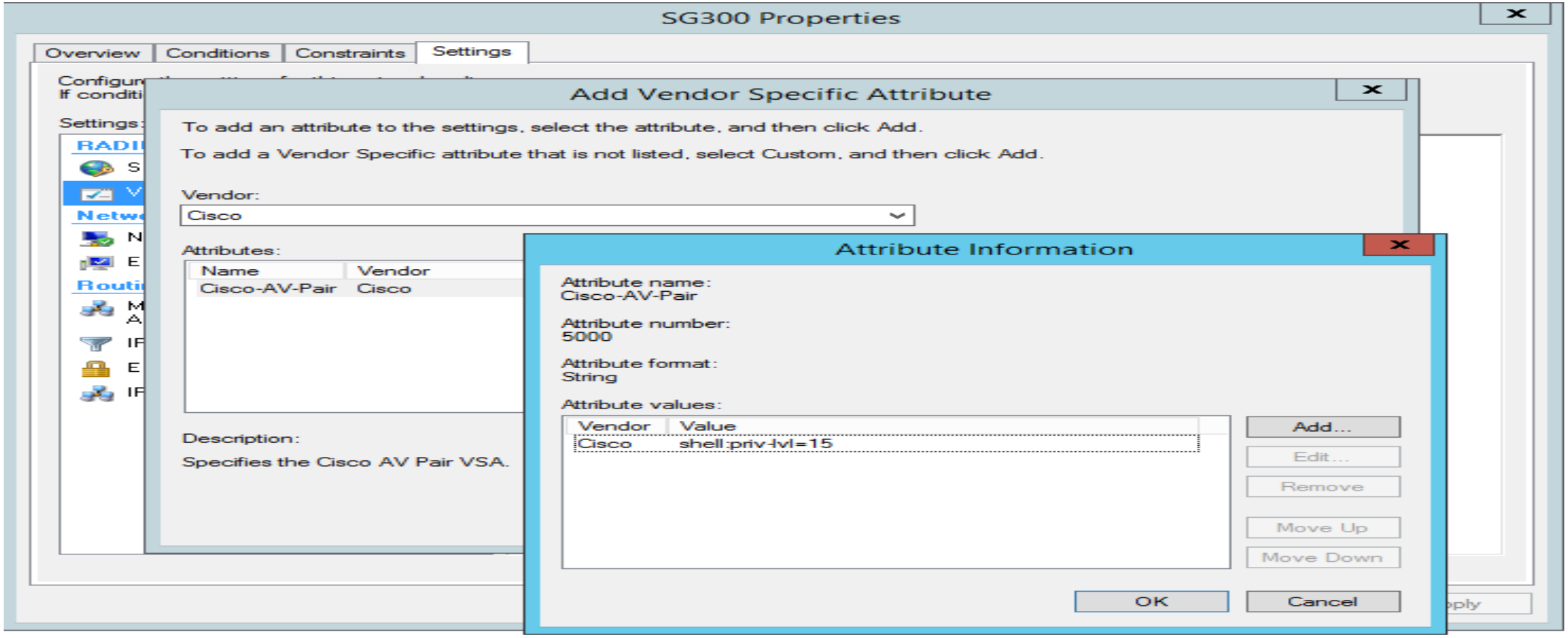


- Select Vendor Specific on the left then click Add
- Select Cisco for Vendor then click Add
- Click Add again and enter shell:priv-lvl=15

For Small Business

cisco

9. Network Policies – Settings * Vendor



- Select Vendor Specific on the left then click Add
- Select Cisco for Vendor then click Add
- Click Add again and enter shell:priv-lvl=15

For Small Business

cisco