



For
Small
Business



Windows Server NPS (Radius) with SMB Switches

Authentication for GUI, Web and SSH, etc.

Momotombo, Nicaragua

1. Configure Switch Security Setting (Radius)

The screenshot shows the configuration page for RADIUS on a Cisco SF300-24MP switch. The left sidebar shows the navigation menu with 'Security' expanded and 'RADIUS' selected. The main content area is titled 'RADIUS' and includes a warning: 'RADIUS Accounting for Management Access can only be enabled when TACACS+ Accounting is disabled. TACACS+ Accounting is currently disabled.'

RADIUS Accounting:

- Port Based Access Control (802.1X, MAC Based)
- Management Access
- Both Port Based Access Control and Management Access
- None

Use Default Parameters:

- Retries: 3 (Range: 1 - 10, Default: 3)
- Timeout for Reply: 3 sec (Range: 1 - 30, Default: 3)
- Dead Time: 0 min (Range: 0 - 2000, Default: 0)

Key String:

- Encrypted: Mai8NuONauUuNZpj€
- Plaintext: (0/128 characters used)

Source IPv4 Interface: Auto

Source IPv6 Interface: Auto

RADIUS Table:

Server	Priority	Key String (Encrypted)	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
<input type="checkbox"/> 192.168.0.55	1	Mai8NuONauUuNZ...	3*	1812	1813	3*	0*	Login

Buttons: Add..., Edit..., Delete

Footer: An * indicates that the parameter is using the default global value. Display Sensitive Data as Plaintext

You can use either Management Access or Port Based Access Control

We need to add a new RADIUS Server point of contact

2. Fill all the information required for Radius

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface:

* Server IP Address/Name:

* Priority: (Range: 0 - 65535)

Key String: Use Default
 User Defined (Encrypted)
 User Defined (Plaintext) (0/128 characters used)

* Timeout for Reply: Use Default
 User Defined sec (Range: 1 - 30, Default: 3)

* Authentication Port: (Range: 0 - 65535, Default: 1812)

* Accounting Port: (Range: 0 - 65535, Default: 1813)

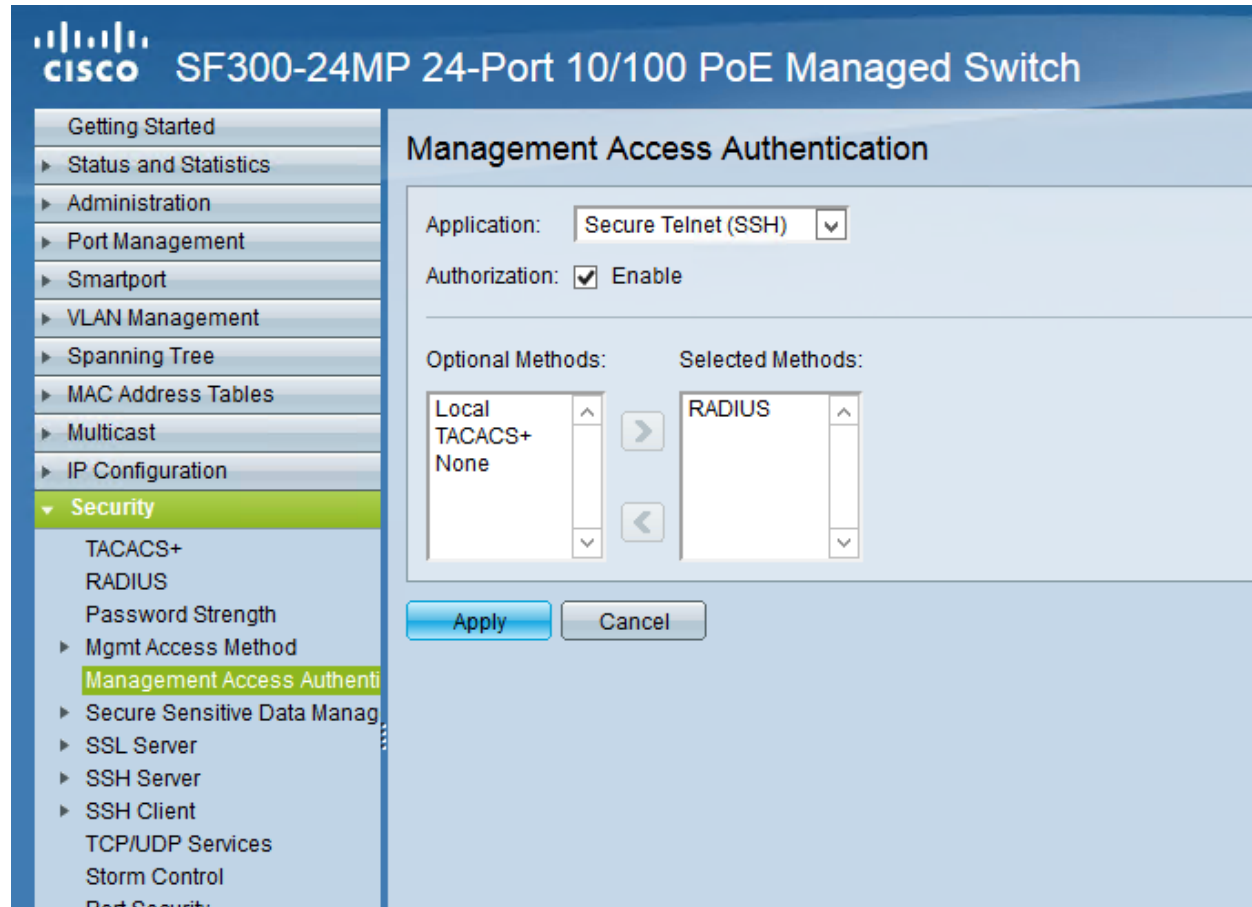
* Retries: Use Default
 User Defined (Range: 1 - 10, Default: 3)

* Dead Time: Use Default
 User Defined min (Range: 0 - 2000, Default: 0)

Usage Type: Login
 802.1x
 All

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

3. Go to “Management Access Authentication”



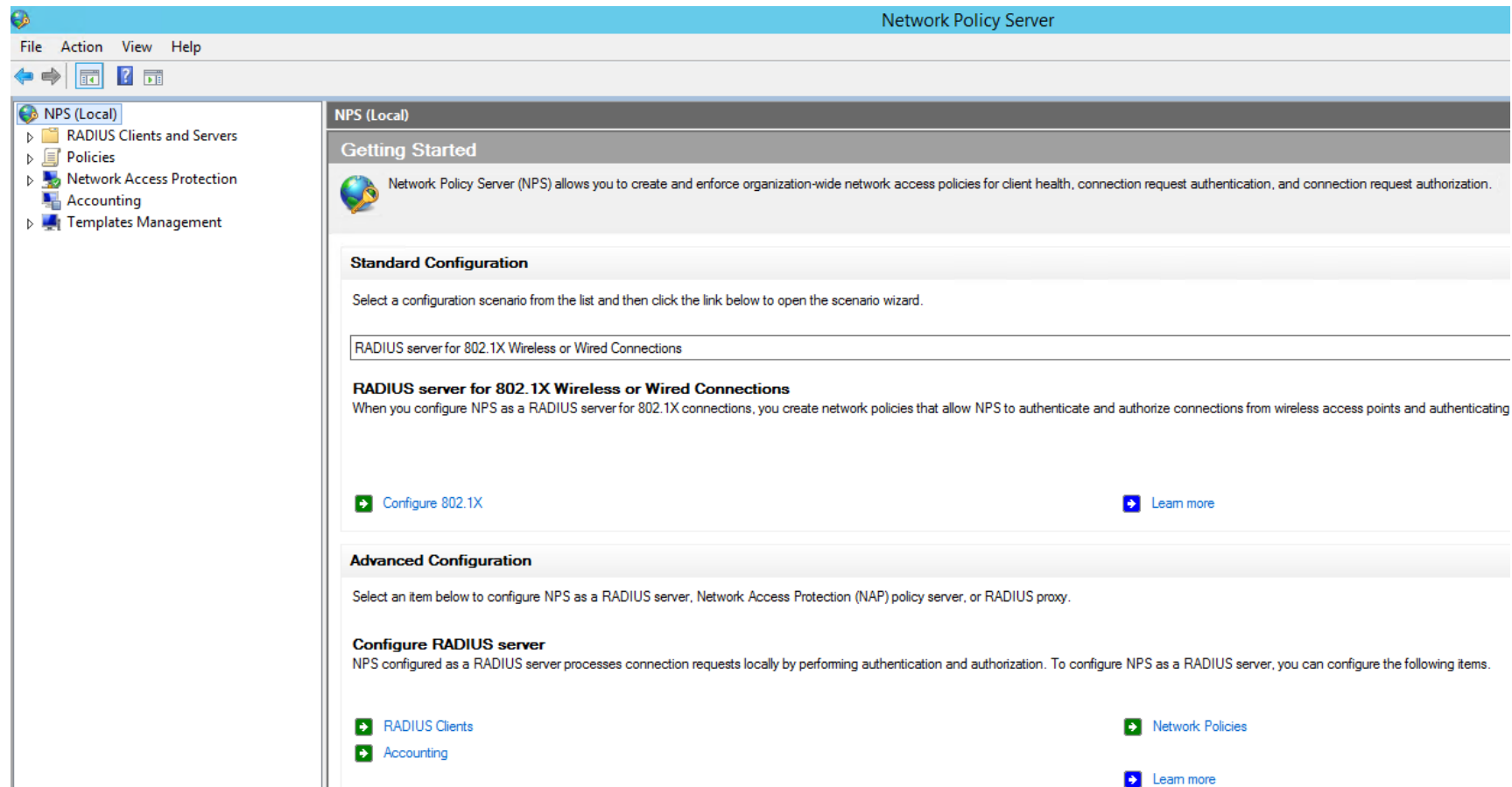
On Application, you can select the access method to evaluate with Radius Server such as:

- 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.

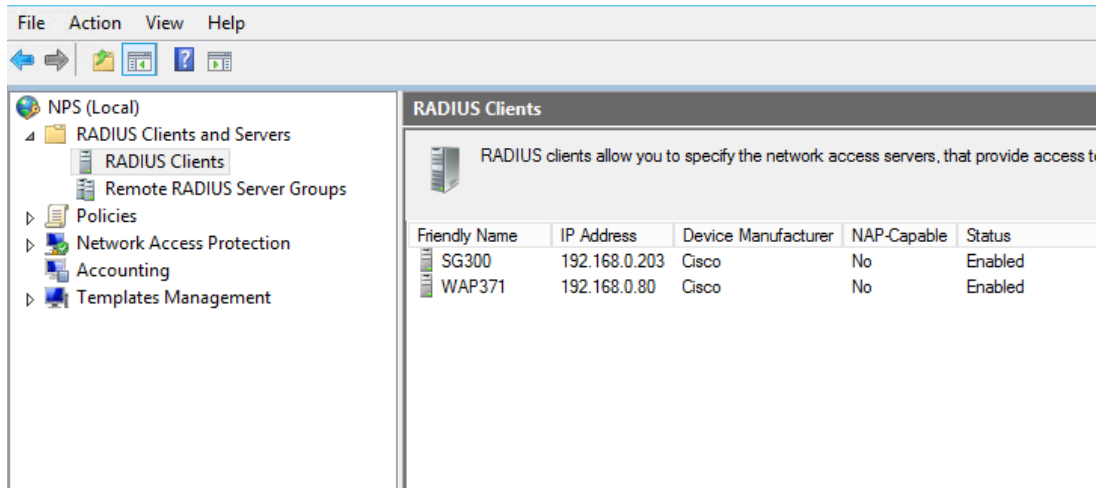
4. Open Windows NPS (Radius Server)



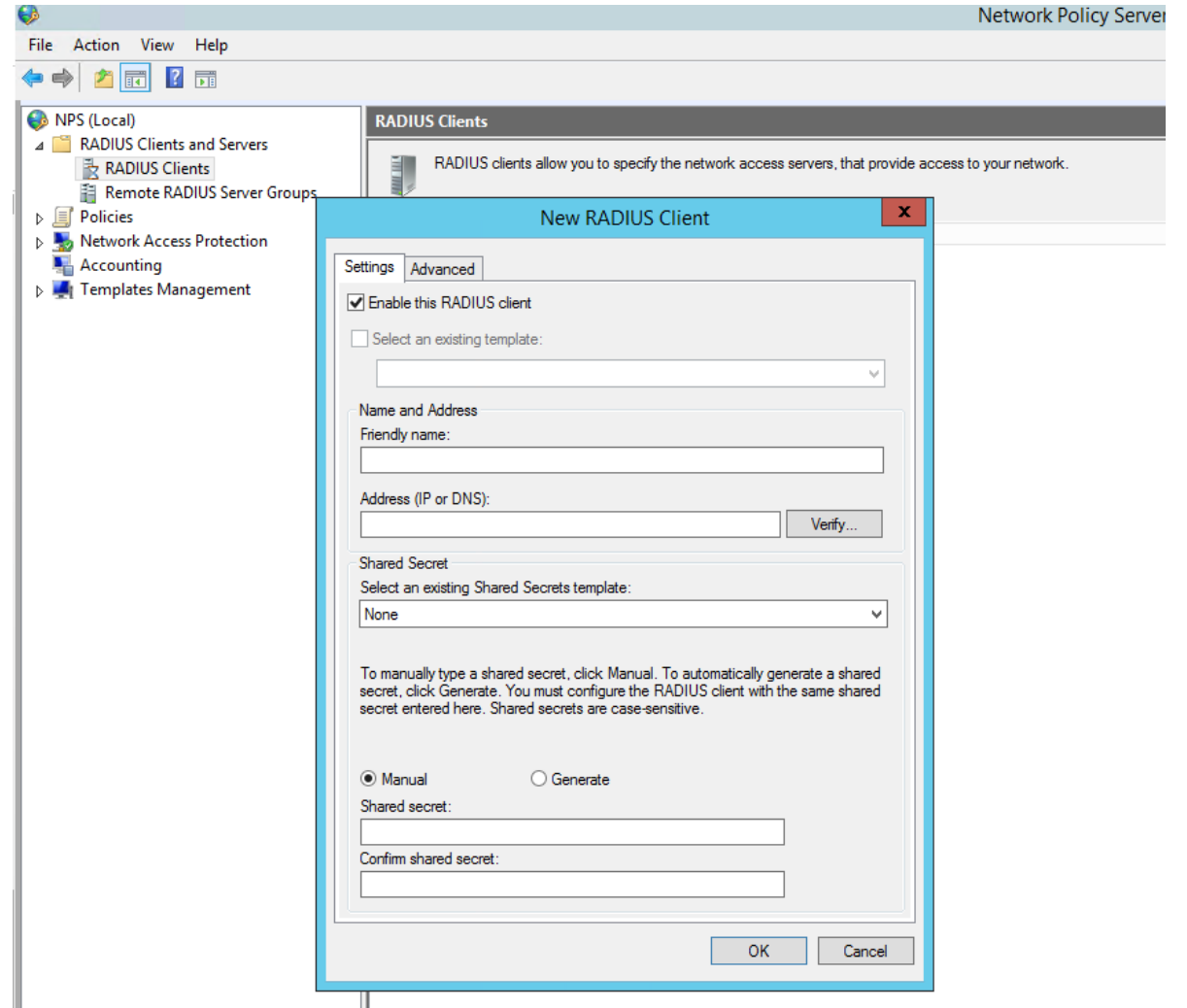
For
Small
Business



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



6. Fill the information for new Radius Client

SG300 Properties

Settings Advanced

Enable this RADIUS client

Select an existing template:

Name and Address

Friendly name:
SG300

Address (IP or DNS):
192.168.0.203

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:
.....

OK Cancel Apply

* Friendly Name is referring to Hostname of the Switch

CISCO SF300-24MP 24-Port 10/100 PoE Managed Switch

Getting Started
Status and Statistics
Administration
System Settings
Console Settings
User Accounts
Idle Session Timeout
Time Settings
System Log
File Management
Reboot
Routing Resources
Diagnostics
Discovery - Bonjour
Discovery - LLDP
Discovery - CDP

System Settings

System Description: SF300-24MP 24-Port 10/100 PoE Managed Switch

System Location: (0/160 characters used)

System Contact: (0/160 characters used)

Host Name:
 Use Default
 User Defined SG300 (5/58 characters used; Default: switchea7246)

System Mode
 L2
 L3

Custom Banner Settings

* 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:

SG300 Properties

Settings Advanced

Vendor
Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

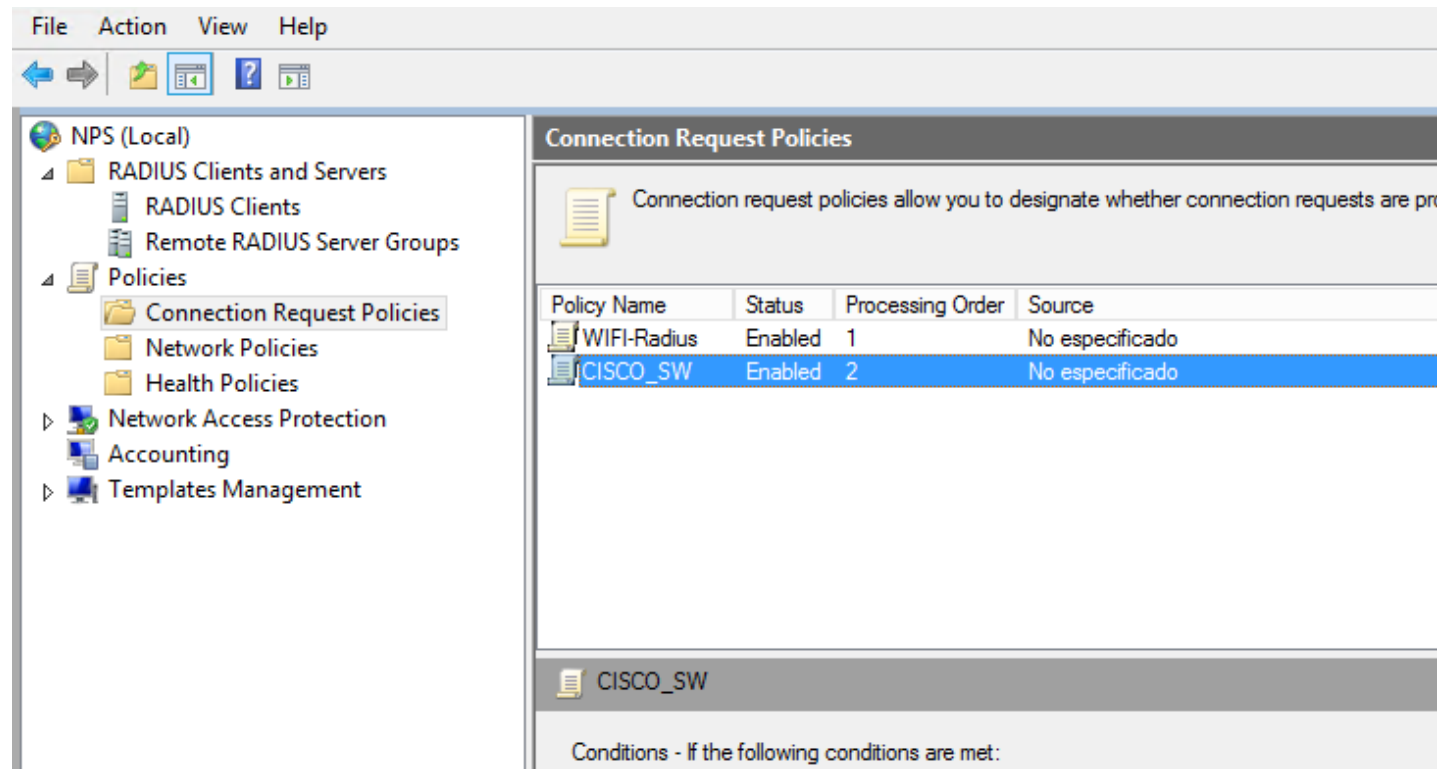
Vendor name:
Cisco

Additional Options

Access-Request messages must contain the Message-Authenticator attribute

RADIUS client is NAP-capable

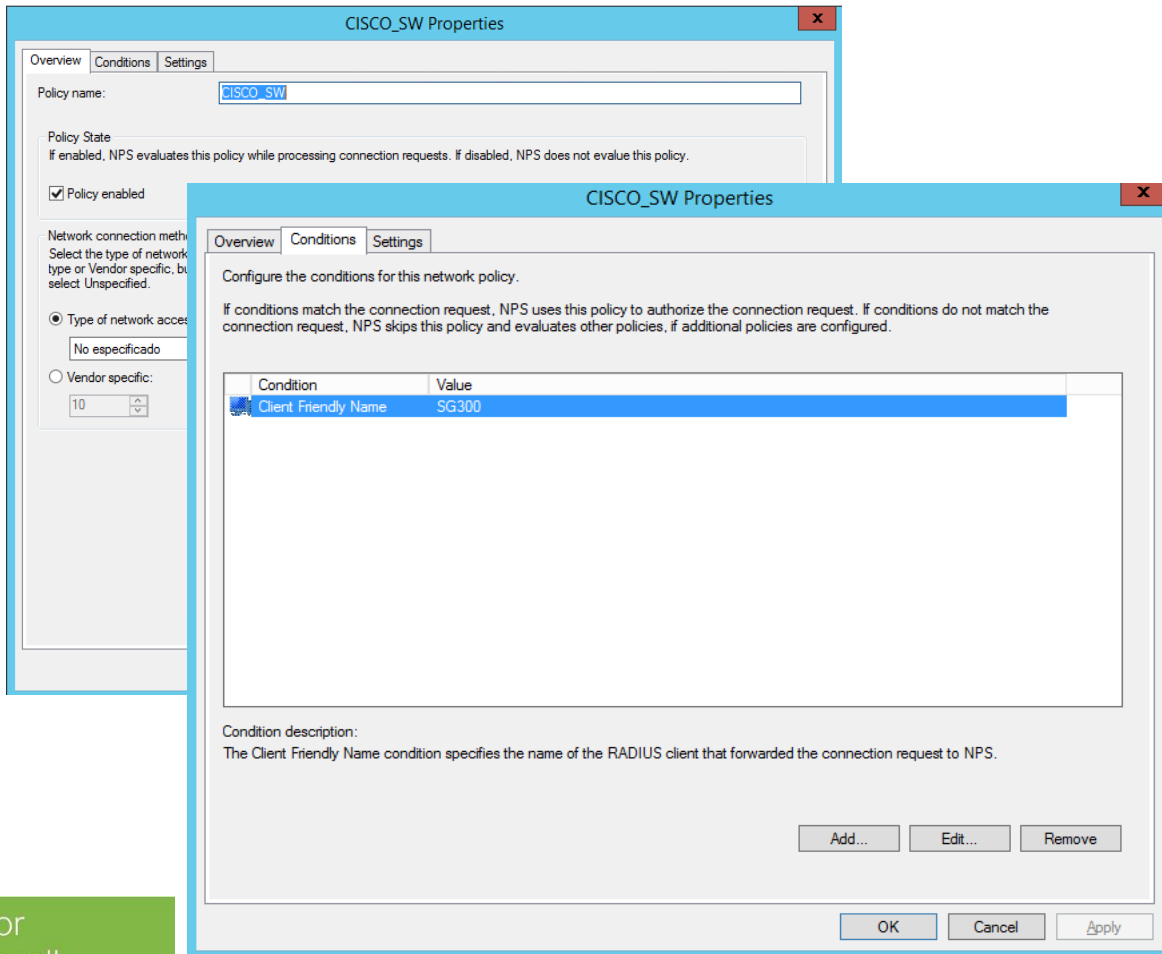
7. Verify Radius Policies



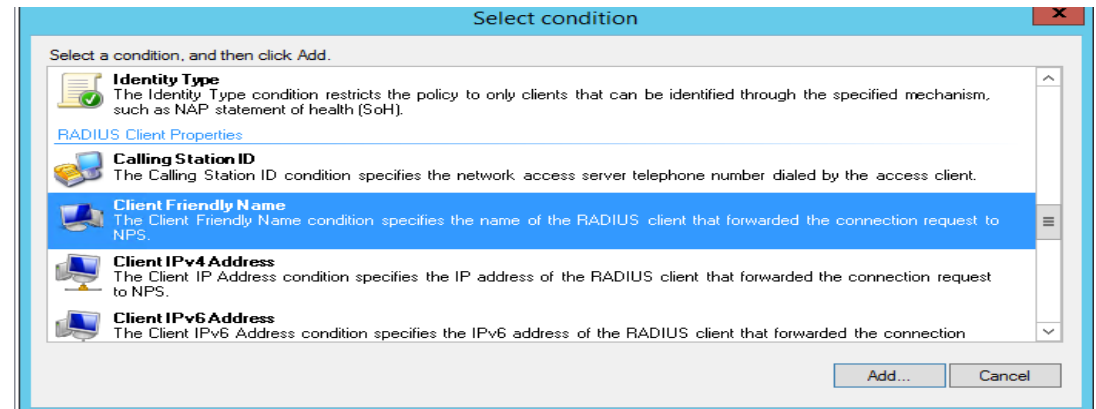
We need to verify two Policies:

1. Connection Request Policies and
2. Network Policies

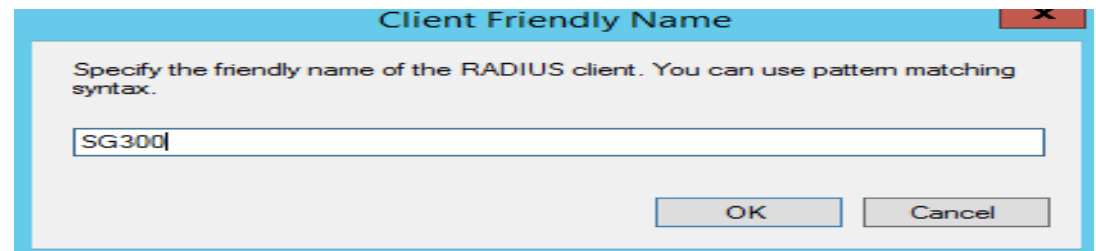
8.A - Create a new Connection Request Policies



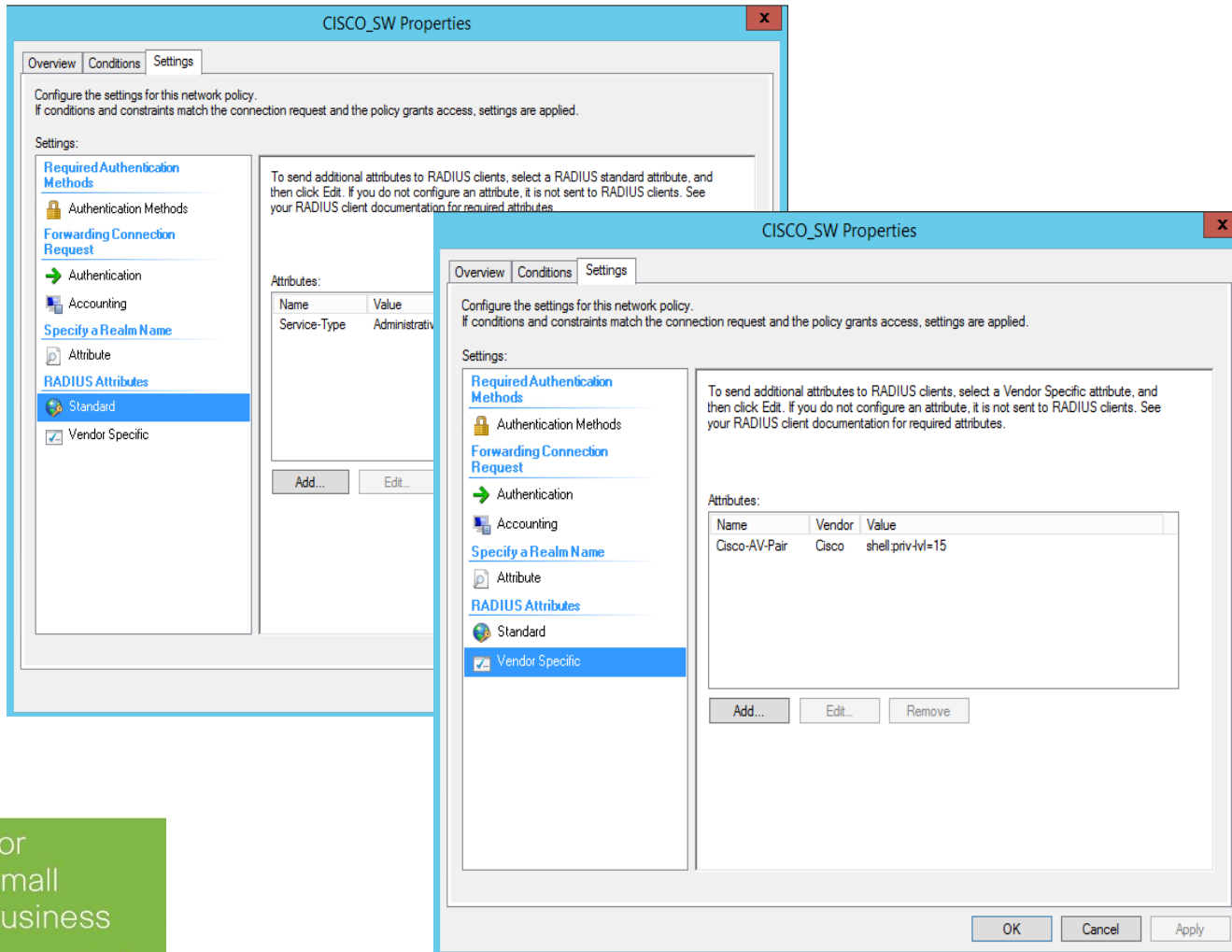
On Conditions tab you need to add a new condition row, just click on Add button and look for the option “Client Friendly Name”



And type the hostname of SW.

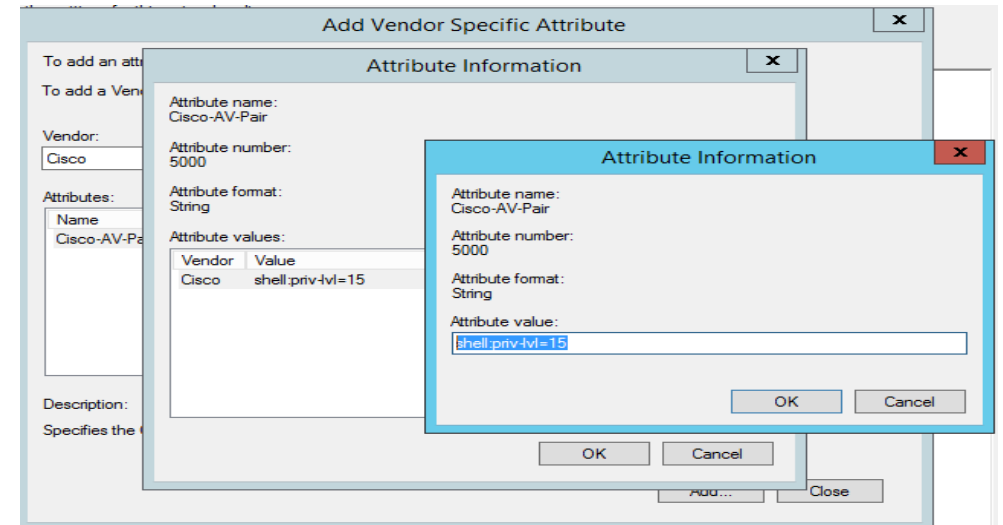


8.B - Verify the Setting tab before save the policy



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



9. Network Policies - Overview

SG300 Properties

Overview Conditions Constraints Settings

Policy name: SG300

Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

Policy enabled

Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

Grant access. Grant access if the connection request matches this policy.

Deny access. Deny access if the connection request matches this policy.

Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.

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.

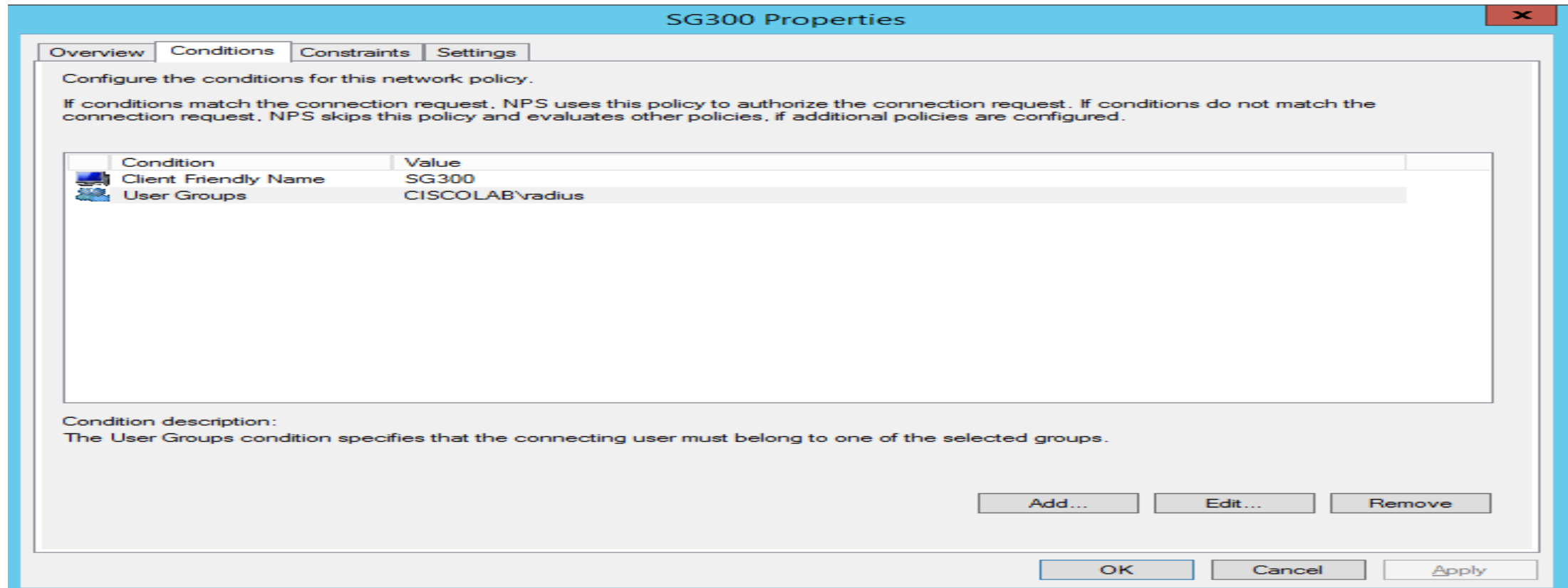
Type of network access server:
No especificado

Vendor specific:
10

OK Cancel Apply

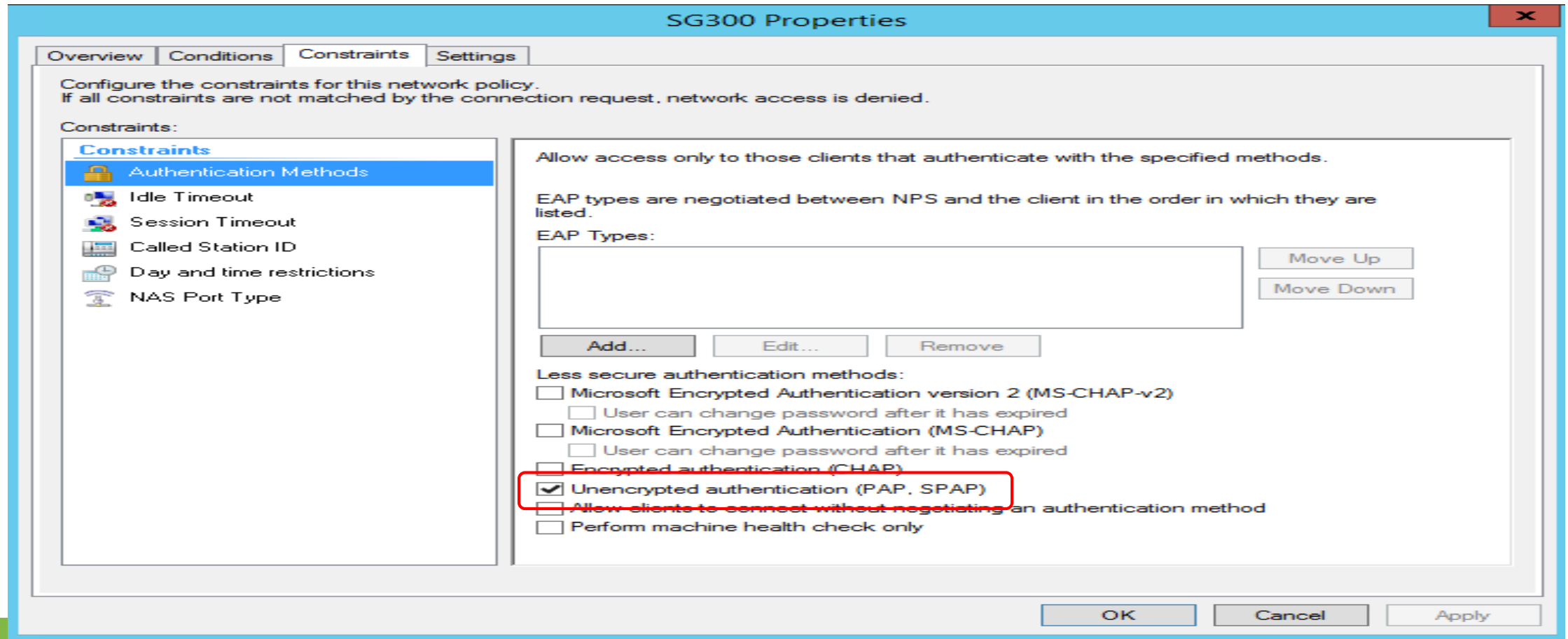
We need to enable the “Ignore user account dial-in properties” option

9. Network Policies - Conditions



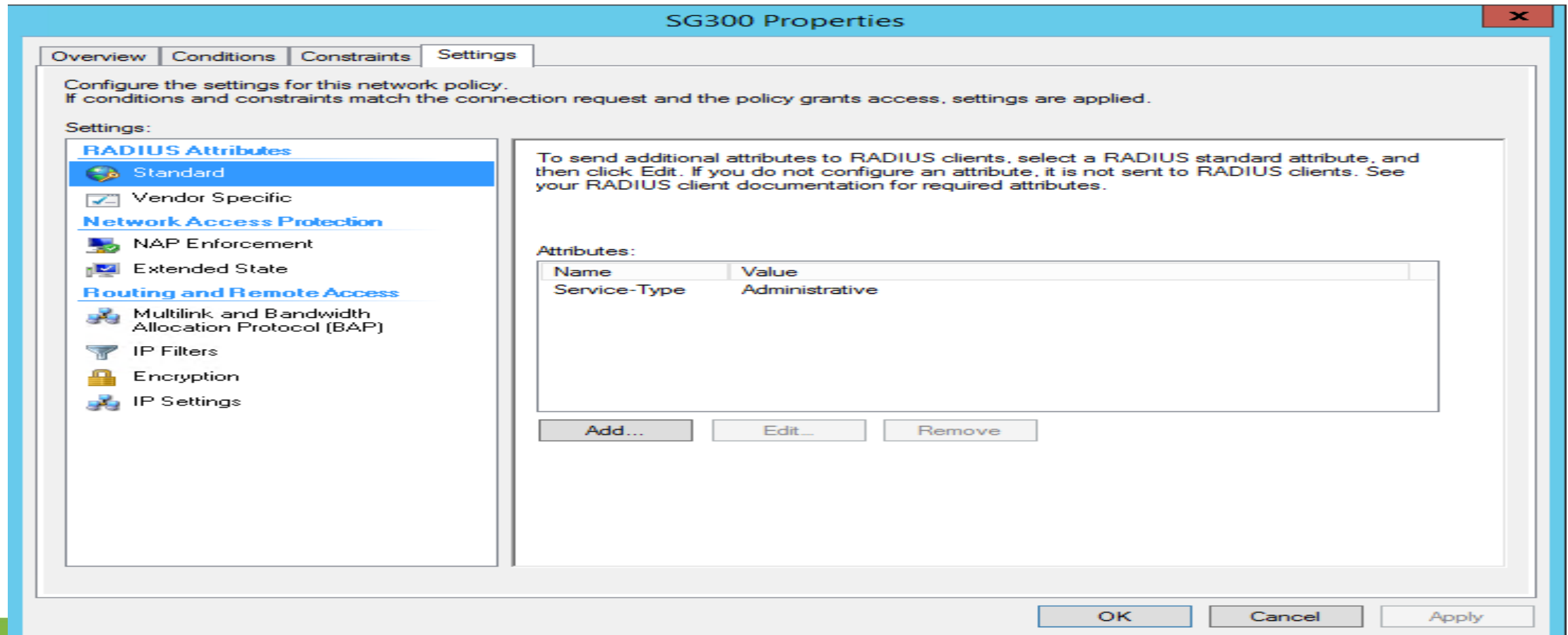
- We need to add:
 - Client friendly name
 - User group to use.

9. Network Policies – Constraints



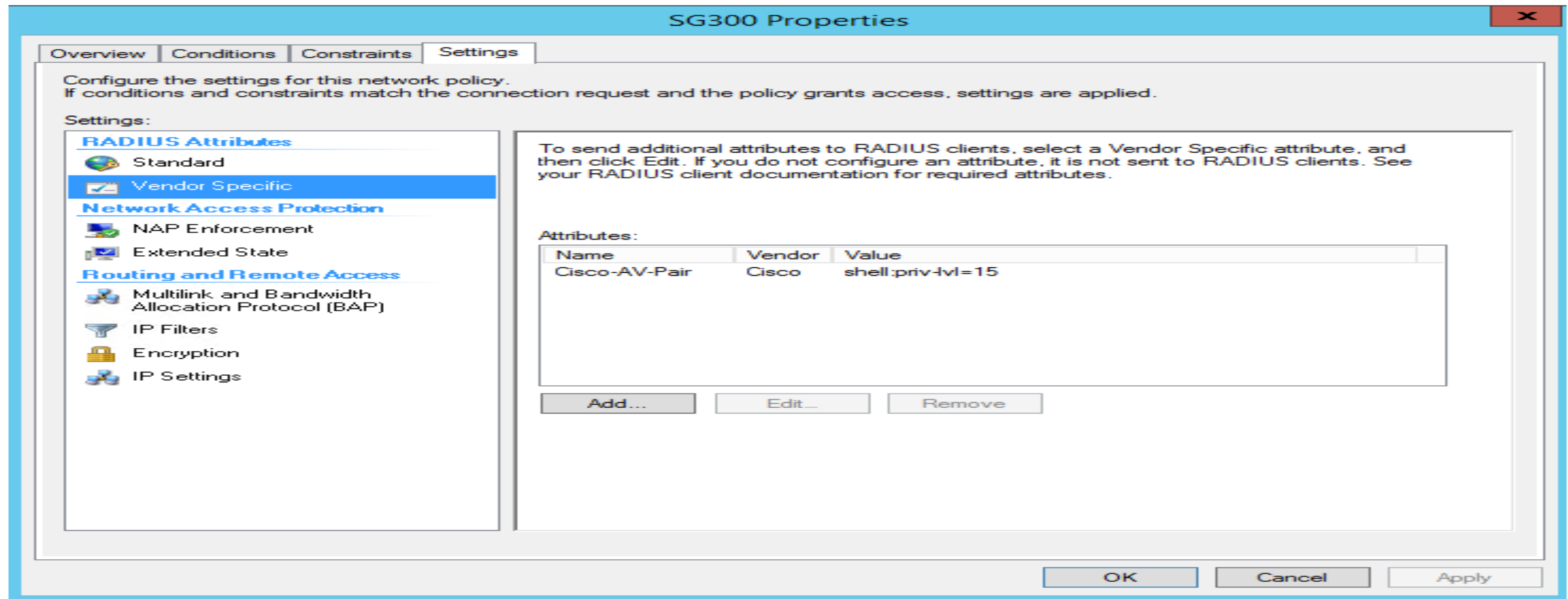
- Uncheck everything then select Unencrypted authentication (PAP, SPAP)

9. Network Policies – Settings



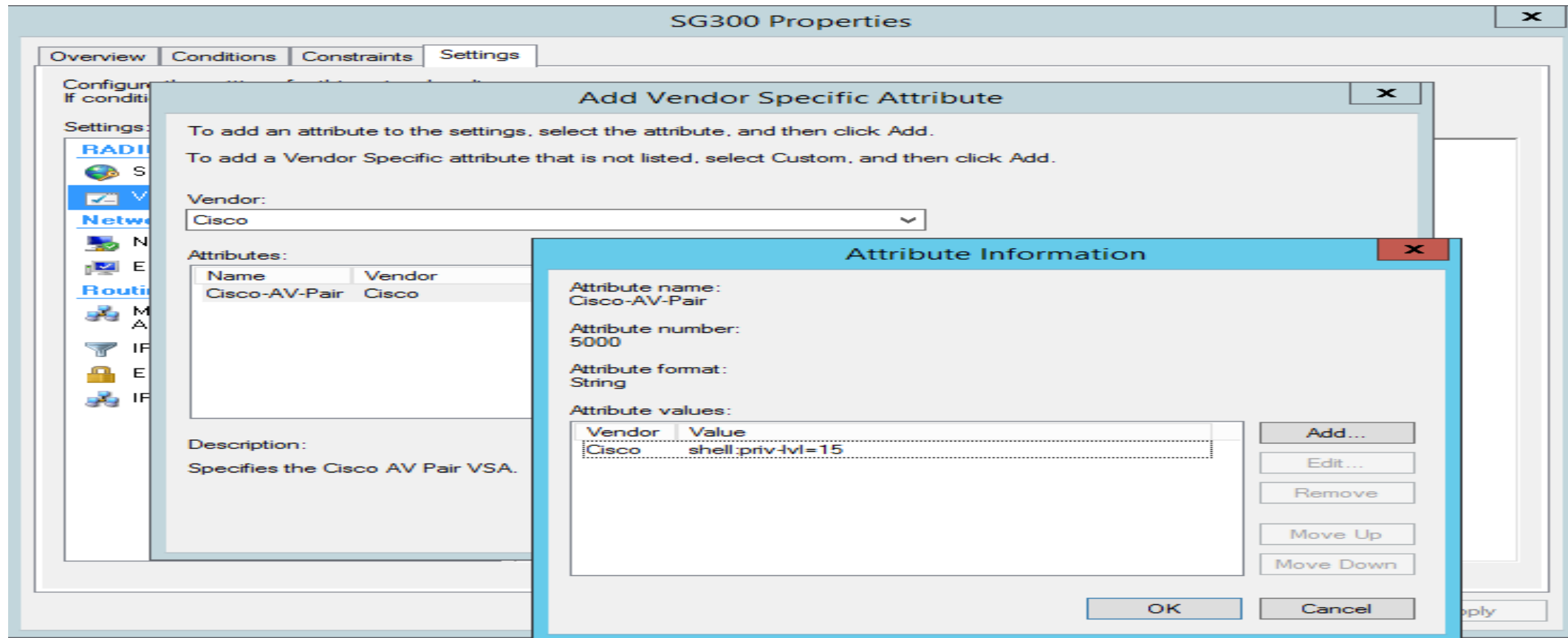
- Select and remove the Framed-Protocol and set Service-Type attributes

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

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