

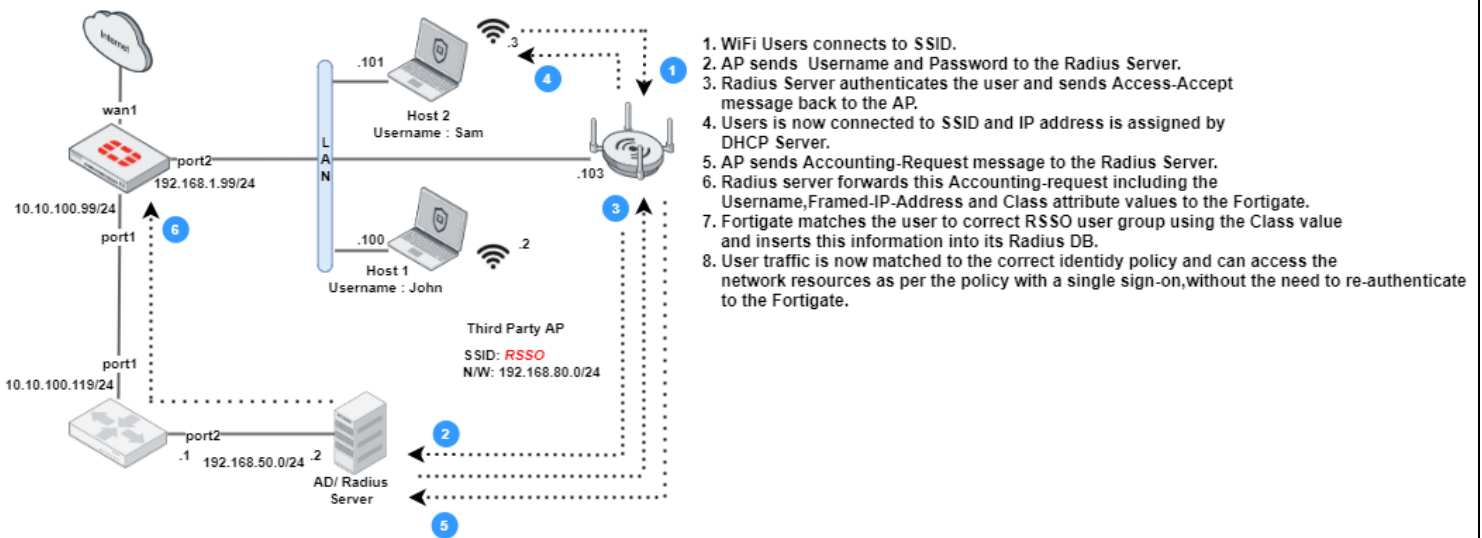
RADIUS SINGLE-ON [RSSO]

When the user is connected to LAN and is successfully authenticated by Active Directory, DC's security event log can be polled for logon events and this information is sent to Fortigate to record the IP address, Username and Group information associated to that event. Users may have a static IP or may have DHCP server assigning the IP address. If this is a laptop, for example, most of the times authentication request are made using the Ethernet interface (default setting). What happens when the user is disconnected from wired connection? Fortigate does not know the IP address of the wireless interface on this laptop and now the user is no longer authenticated to the firewall. User may have to sign out and sign back in to make the authentication request via wireless IP.

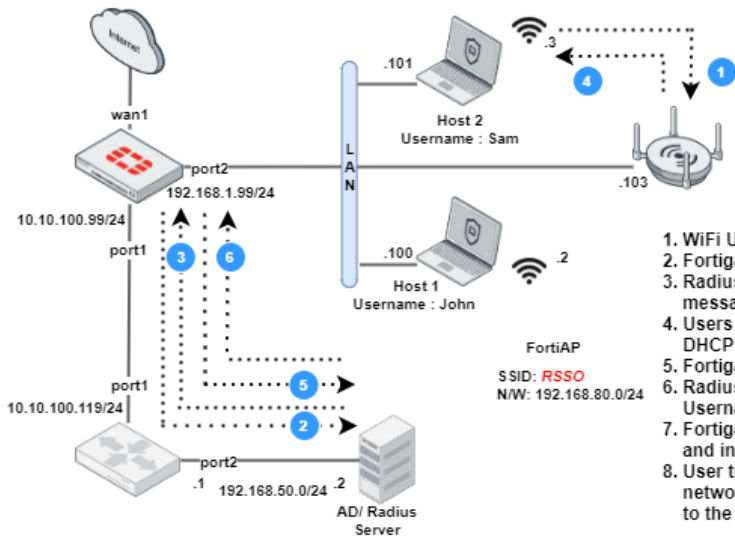
This is where RSSO comes into picture. RSSO uses the wireless authentication(802.1x) request from the Radius server authenticating that request via Radius Accounting. We will discuss more about this in a bit. Typically, RSSO is solution when third party AP is used but that does not restrict the administrator from using this solution with FortiAP.

AUTHENTICATION FLOW:

When third-party AP is deployed:



When FortiAP is deployed: (802.1x is used to authenticate the WiFi users)



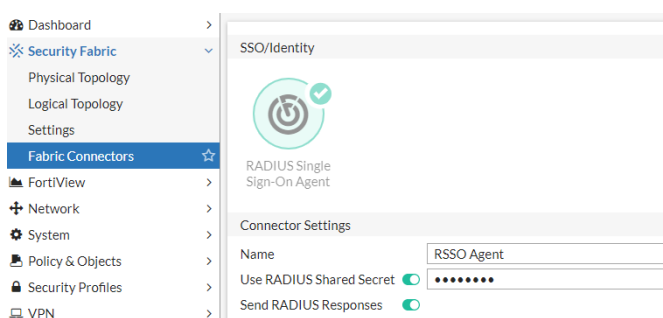
1. WiFi Users connects to SSID.
2. Fortigate(WLC) sends Username and Password to the Radius Server.
3. Radius Server authenticates the user and sends Access-Accept message back to the Fortigate
4. Users is now connected to SSID and IP address is assigned by DHCP Server.
5. Fortigate sends Accounting-Request message to the Radius Server.
6. Radius server forwards this Accounting-request including the Username, Framed-IP-Address and Class attribute values to the Fortigate.
7. Fortigate matches the user to correct RSSO user group using the Class value and inserts this information into its Radius DB.
8. User traffic is now matched to the correct identity policy and can access the network resources as per the policy with a single sign-on, without the need to re-authenticate to the Fortigate.

The configuration components we will be working are show below:

1. RSSO Accounting Listener which listens on port 1813 for accounting packets
2. Radius Accounting and Fortigate Radius Server
3. Configuring RSSO user group
4. Configuring WiFi SSID
5. Configuring NPS (Windows server 2019) for authentication and authorization

RSSO Accounting Listener which listens on port 1813 for accounting packets

1. Login to the Fortigate and Click on Security Fabric > Fabric Connectors > Create New and select “Radius Single Sign-On Agent”
2. Enable “Use RADIUS Shared Secret” and provide the Shared Secret configured in the NPS
3. Enable “Send RADIUS Responses” and click on OK



```
config user radius
  edit "RSSO Agent"
    set rspo enable
    set rspo-radius-response enable
    set rspo-validate-request-secret enable
    set rspo-secret ENC TAlcudAKY2tuXjhXTjRK0sgZ
    set rspo-endpoint-attribute User-Name
    set rspo-context-timeout 0
    set rspo-flush-ip-session enable
  next
end
```

4. Connect to the CLI and add the above show configuration to the “RSSO Agent”

Please note that the FortiAP uses the attribute “User-Name” to denote the user. Please refer to other vendor’s documentation for corresponding attribute for this field in their accounting packets.

“rsso-context-timeout” can be used to clear authentication after ‘x’ number of seconds (when set to 0, it never times out)

Radius Accounting and Fortigate Radius Server

1. Create radius server on the Fortigate and enable "Radius Accounting" on the interface connecting to the NPS.

Edit RADIUS Server

Name: NPS

Authentication method: Default **Specify**

NAS IP: MS-CHAP-v2

Include in every user group:

Primary Server

IP/Name: 10.10.100.119

Secret: ••••••••

Connection status: Successful

Test Connectivity

Test User Credentials

```
config user radius
edit "NPS"
set server "10.10.100.119"
set secret ENC ZuFofpwEhC5IM2U1my9fRVa
set auth-type ms_chap_v2
config accounting-server
edit 1
set status enable
set server "10.10.100.119"
set secret ENC l+1ifvZM2N9COO3
set source-ip "10.10.100.99"
next
end
next
end
```

2. From the CLI, add the above show configuration to send accounting packets for any connection that uses this server.
3. Accounting packets will now be sent to port 1813 of the radius server

Configuring RSO user group

1. From User & Device > User Group, Click Create New
2. Provide the name for the group and select "Radius Single Sign-On(RSSO)"
3. Enter the "Radius Attribute Value" for this group. This is the value which the NPS should send to Fortigate (sent in HEX) and Fortigate will use this value to map the correct group and identity policy.

New User Group

Name: Restricted

Type: Firewall
Fortinet Single Sign-On (FSSO)
RADIUS Single Sign-On (RSSO)
Guest

RADIUS Attribute Value ⓘ: Restrict

OK Cancel

Configuring WiFi SSID

1. Click on WiFi & Switch Controller > SSID > Create New SSID
2. Provide name for the interface, IP/Netmask and enable DHCP Server
3. Enter the name for the SSID and select “WPA2 Enterprise”
4. Now for the authentication select “Radius Server” and choose the Radius server created earlier in this article and click OK

The screenshot displays the 'WiFi Settings' configuration page. The 'SSID' field is set to 'do not connect'. The 'Security mode' is set to 'WPA2 Enterprise'. The 'Client limit' is disabled. Under 'Authentication', 'Local' is disabled and 'RADIUS Server' is selected. The 'NPS' server is chosen from the dropdown. 'Dynamic VLAN assignment' is disabled. 'Broadcast SSID' is enabled. The 'Schedule' is set to 'always'. 'Block intra-SSID traffic' is disabled. Under 'Broadcast suppression', 'ARPs for known clients', 'DHCP unicast', and 'DHCP uplink' are all enabled.

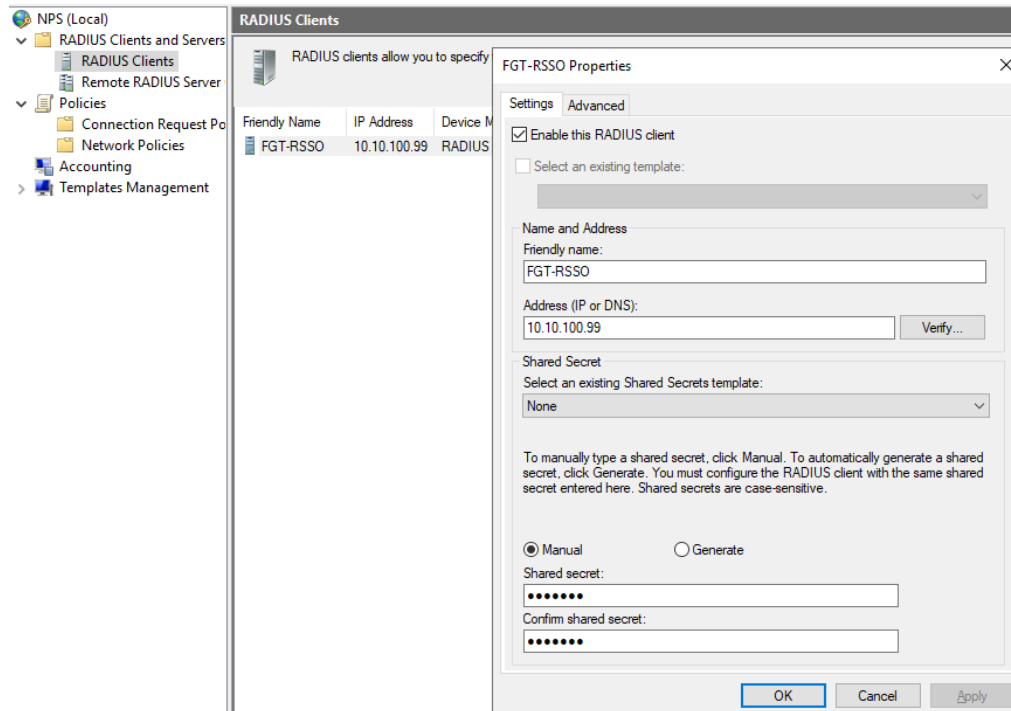
Before proceeding with the NPS configuration, I would like to explain a bit about Protected EAP. Protected EAP with MS-CHAPv2 is an EAP type which is more easily deployed with EAP-TLS or PEAP-TLS because user authentication is accomplished by using password-based credentials (an AD Username and Password) instead of digital certificates or smart cards. Only server running the NPS are required to have a certificate (we will see this in the NPS configuration). Administrator can choose not to use “Server Validation” in the wireless properties in the end-user’s pc, however that is not recommended. When “Server Validation” is enabled, NPS will present its certificate to the client and the client after examining the certificate will have to Trust it. This certificate used by NPS can be issued by a public CA or by the private trust root CA deployed in the network.

Configuring NPS (Windows server 2019) for authentication and authorization

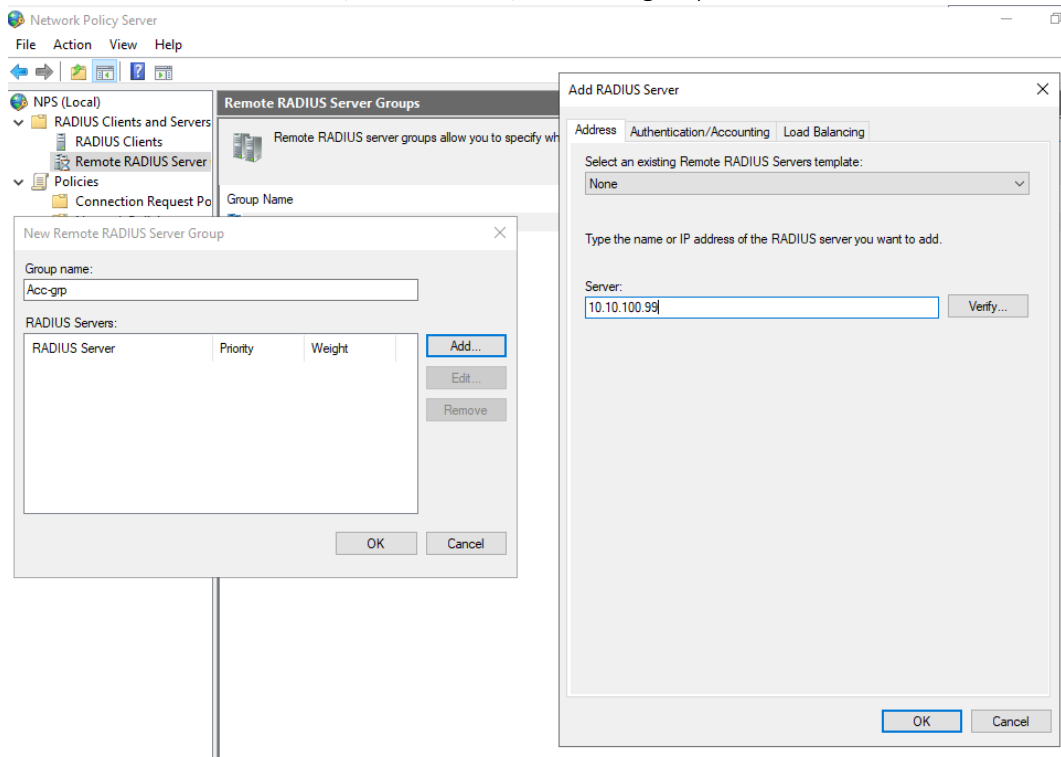
Goal here is to authenticate user and return the correct attribute based on user group membership and forward the Radius Accounting packets to Fortigate for RSO.

Client and Remote Radius Server Group Configuration.

1. Make sure the NPS service is started and registered to the Active Directory
2. Right-Click on "Radius Clients", select New and populate the fields – Friendly Name, Address (Fortigate IP) and shared secret which must match Fortigate Radius server/RSSO agent configuration



3. Right-Click "Remote RADIUS Server", select "New", enter the group name and click on "Add"



4. Use the IP Address of the Fortigate Interface that was configured to listed for “Radius Accounting” in the previous step
5. Navigate to “Authentication/Accounting” tab:
 - a. Un-check “Use the same shared secret for the authentication and accounting”
 - b. Enter the shared secret configured on the forigate for the Radius server/Rsso Agent and click OK

Edit RADIUS Server ×

Address **Authentication/Accounting** Load Balancing

Authentication port:

Select an existing Shared Secrets template:

Shared secret:

Confirm shared secret:

Request must contain the message authenticator attribute

Accounting

Accounting port:

Use the same shared secret for authentication and accounting.

Select an existing Shared Secrets template:

Shared secret:

Confirm shared secret:

Forward network access server start and stop notifications to this server

Configuring Connection Request Policy

1. Right-Click on “Connection Request Policy” and select New
2. Provide a name for the policy and navigate to “Conditions” tab by clicking “Next”

New Connection Request Policy

Specify Connection Request Policy Name and Connection Type
You can specify a name for your connection request policy and the type of connections to which the policy is applied.

Policy name:
RSSO-POLICY-CONNECTION

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:
Unspecified

Vendor specific:
10

Previous Next Finish Cancel

3. Click “Add” and select a condition. Adding “Client IPv4 Address” binds this connect policy to the network policy in the next step. Provide the IP address of the Fortigate and Click ‘OK’ and “Add”

Network Policy Server

File Action View Help

NPS (Local)

- RADIUS Clients and Services
 - RADIUS Clients
 - Remote RADIUS Services
- Policies
 - Connection Request Policies
 - Network Policies
 - Accounting
 - Templates Management

New Connection Request Policy

Specify Connection Request Policy Name and Connection Type

Conditions:

Condition

Condition description:

Add... Edit... Remove

Previous Next Finish Cancel

Select condition

Select a condition, and then click Add.

- Day and Time Restrictions
Day and Time Restrictions are based on the day and time of the connection request.
- RADIUS Client Properties
- Calling Station ID
The Calling Station ID condition specifies the network access server telephone number dialed by the access client.
- Client Friendly Name
The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connection request to NPS.
- Client IPv4 Address**
The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.
- Client IPv6 Address

Client IPv4 Address

Specify the IPv4 address of the RADIUS client. You can use pattern matching syntax.


10.10.100.99

OK Cancel

Add... Cancel

- Next step in to Specify the Connection Request Forwarding. For Authentication, leave as default (Authenticate requests on this server). Click Accounting and check “Forward accounting requests to this remote RADIUS server group” and the select the remote radius server group created earlier. Click on Next.

New Connection Request Policy ✕



Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

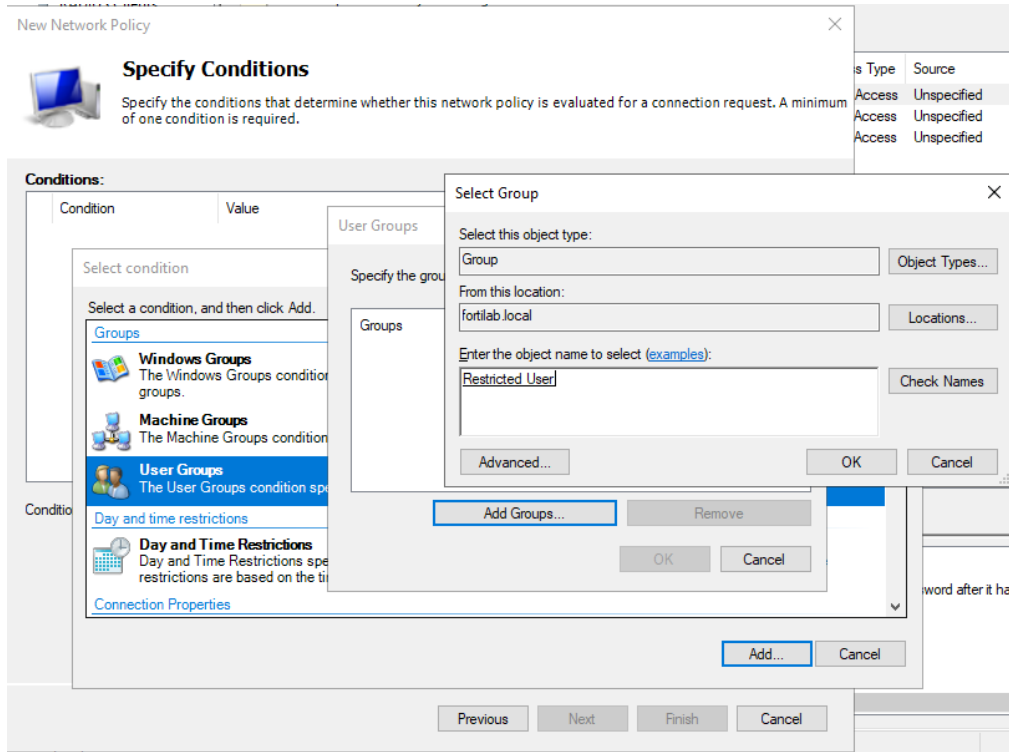
Forwarding Connection Request	RADIUS accounting allows you to record user authentication and accounting requests in a log file or to a SQL Server database. To forward accounting requests to remote RADIUS servers, specify a remote RADIUS server group.
→ Authentication	
Accounting	<input checked="" type="checkbox"/> Forward accounting requests to this remote RADIUS server group
	Acc-grp New...

Previous **Next** Finish Cancel

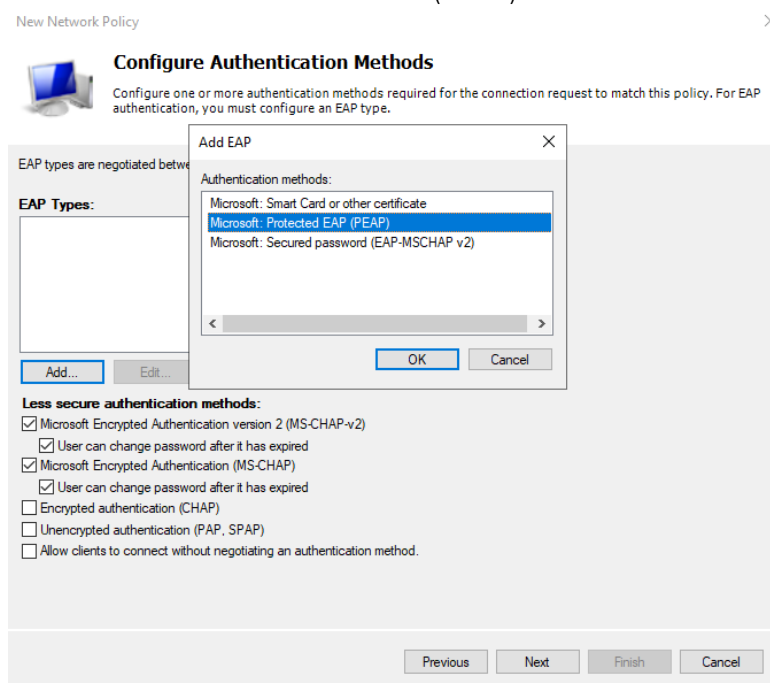
- Leave Specify Authentication Methods to default and Click on Next
- Click Next on Configure Settings dialogue
- Click Finish on the Completing connection request policy

Configuring Network Policies

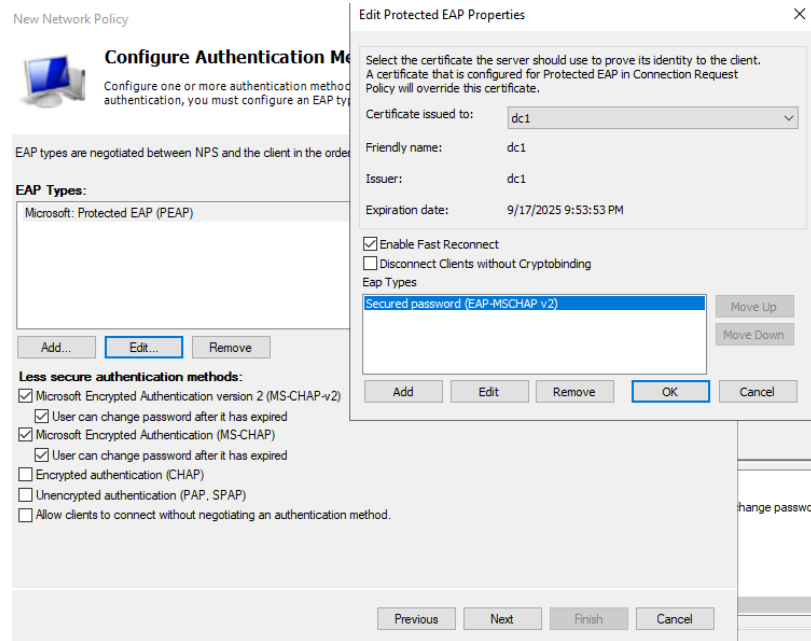
1. Right-Click on “Network Policies” and select New
2. Provide a name for the policy and navigate to “Conditions” tab by clicking “Next”
3. Click “Add” and select a condition. Select “User Groups” and the group for the restricted users. Click OK and Add.



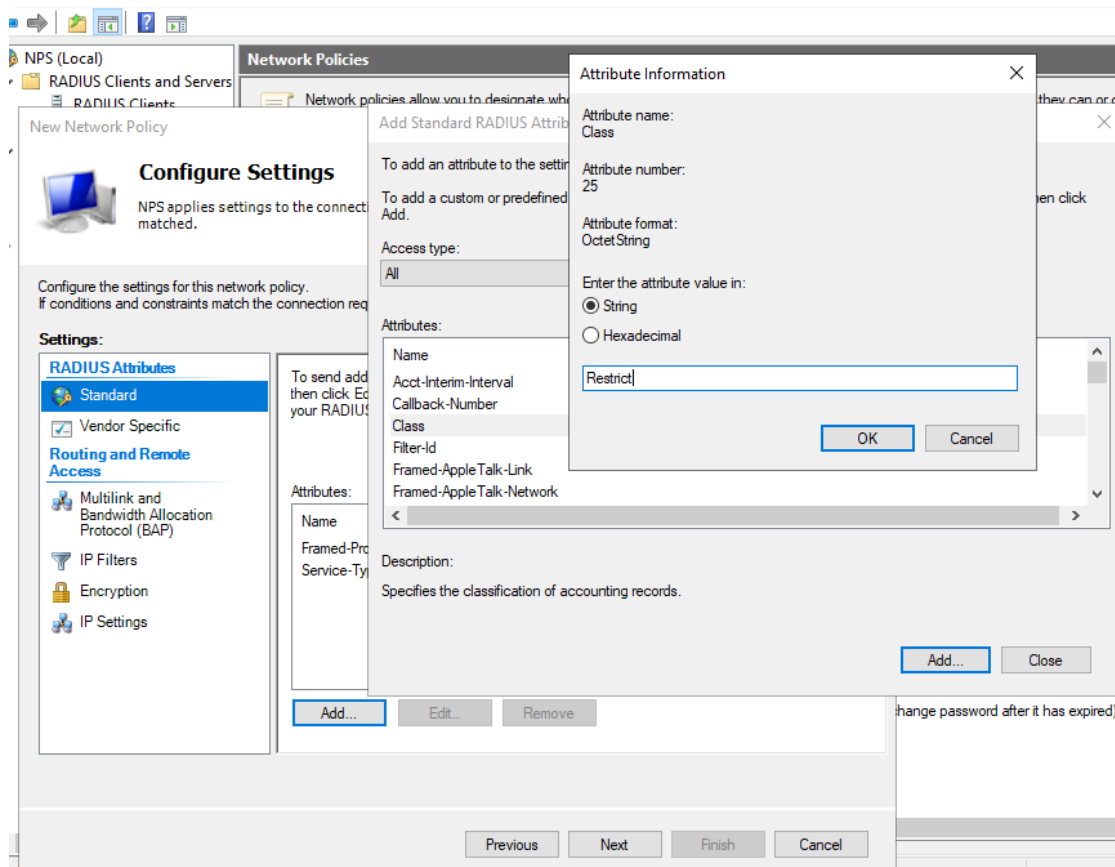
4. Leave Specify Access Permission to default (Access Granted) and click on Next
5. Next few steps are important because this is where the NPS certificate is linked. In the configure Authentication Methods page-
 - a. Select Add and Click on Protect EAP (PEAP)



- b. Click on PEAP and click on Edit, select the certificate that the server should use to prove its identity to the client.



6. Leave Configure Constrains to default
7. In Configure settings, Add a **Standard Radius Attribute – Class**, provide the value for the string. This value should match the sso attribute value in the rso user group. (case-sensitive). Click OK>Add>Next.



8. Verify and click on Finish.