Microsoft NPS Integration Guid

Configuring a Microsoft RADIUS server provides superior authenticati
security: enables group policy enforcement for network segmentation,
and provides record event logs for accounting purposes.

Overview

Configuring a Microsoft RADIUS server provides superior authentication security: enables group policy enforcement for network segmentation, and provides record event logs for accounting purposes.

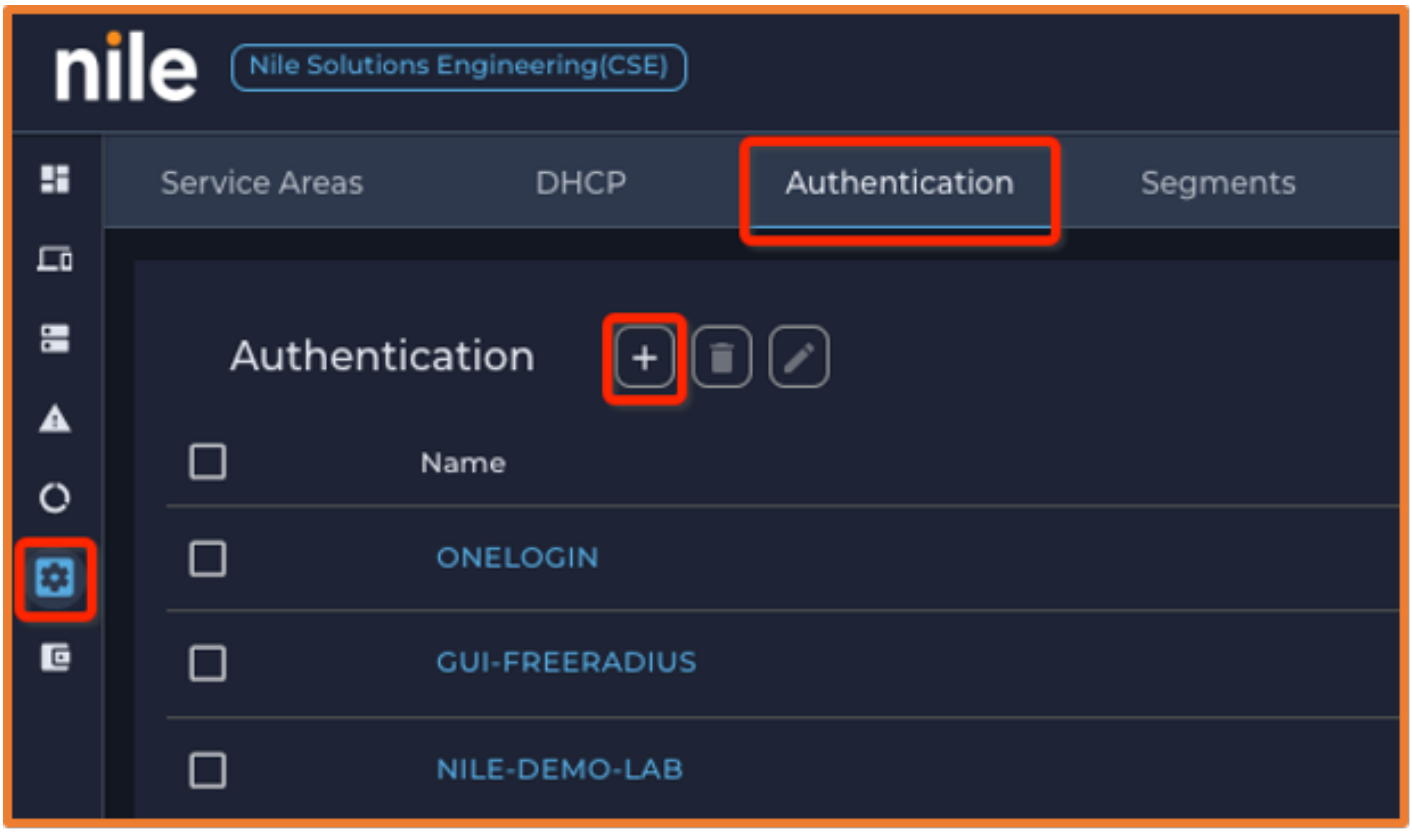
Combining a secure Microsoft RADIUS server with certificate solutions creates a network environment that is strongly protected, and a straightforward experience for users.

Prerequisites

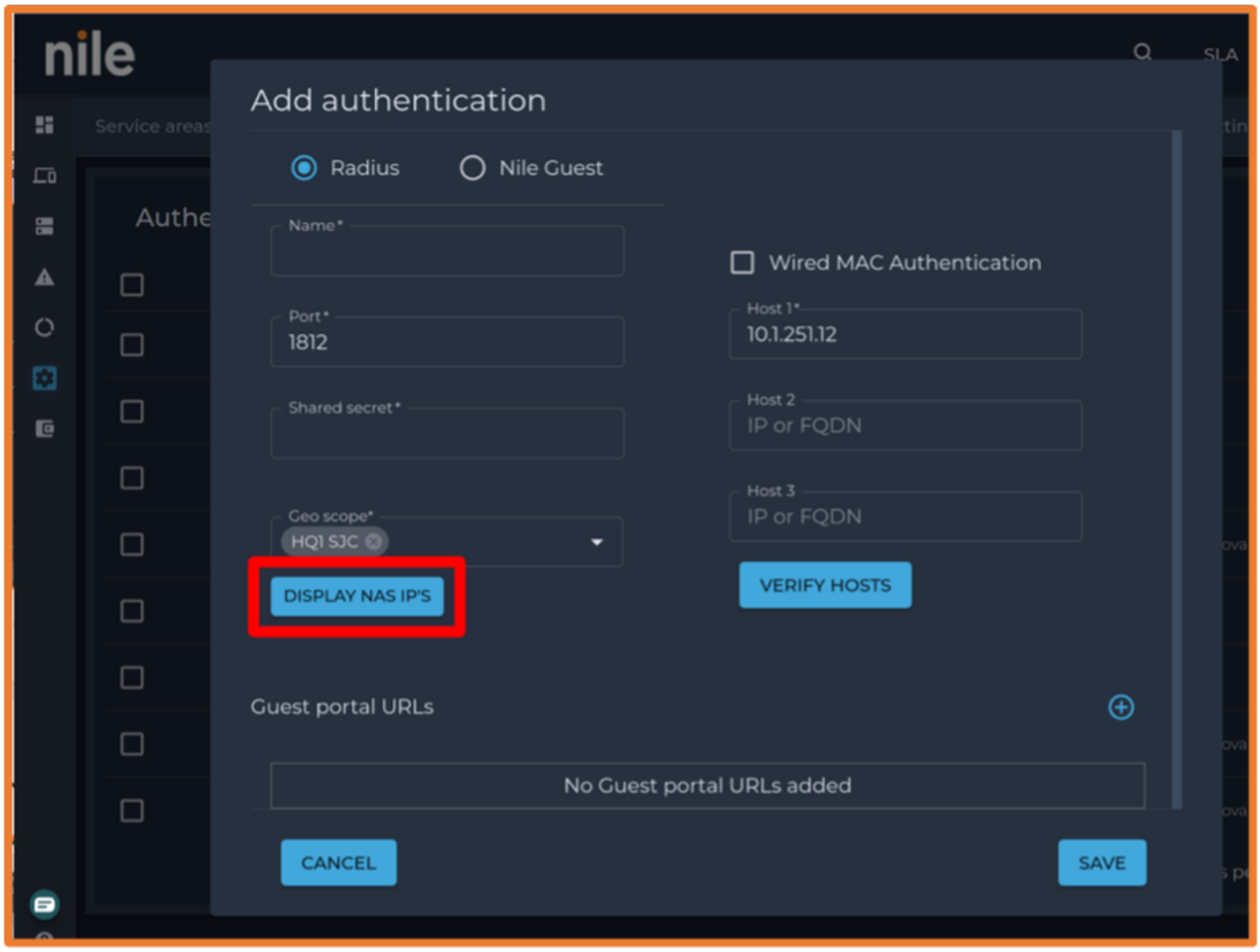
- Microsoft NPS RADIUS Server
- Identity Provider
- Administrator rights to Nile Portal
- Administrator rights to Microsoft NPS

Configuring Nile Authentication Server (RADIUS)

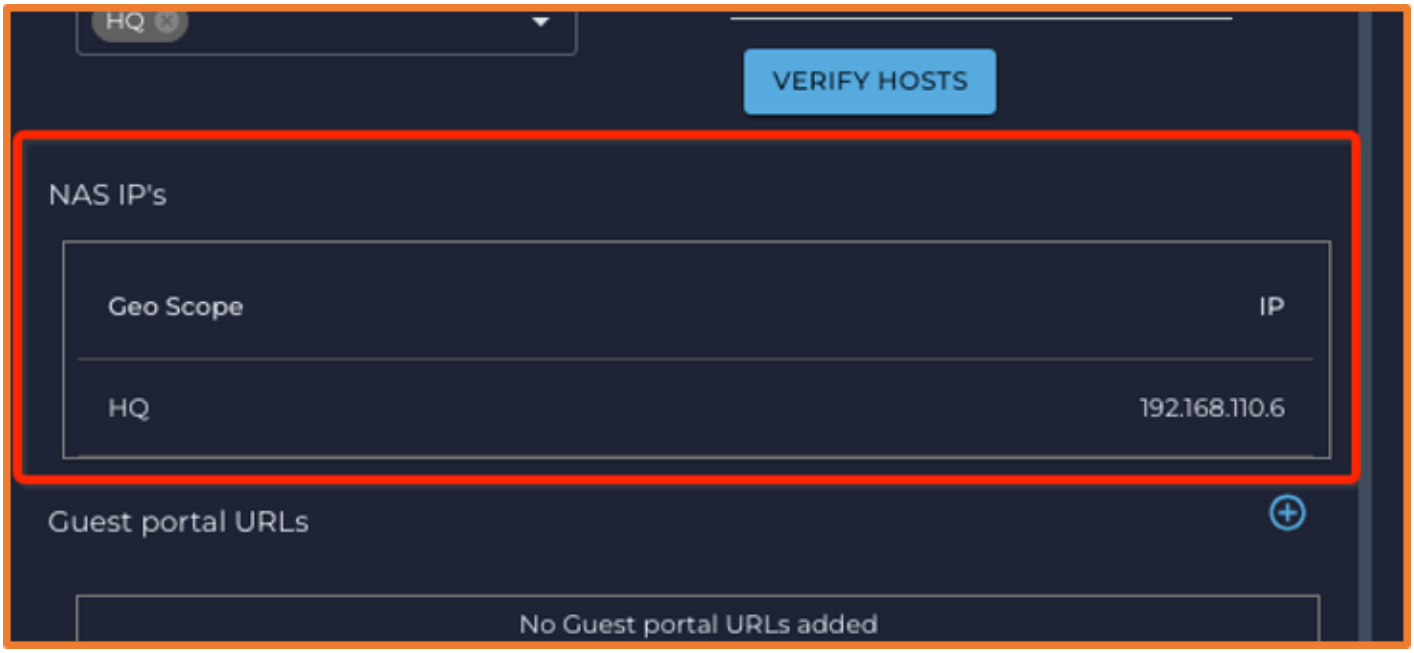
- Log onto Nile Portal: https://u1.nile-global.cloud/
- Navigate to **Nile Portal ® Settings** button **® Authentication** tab
- Click on the + (add authentication button) to create a new Microsoft NPS RADIUS authentication configuration:



- Fill in the Microsoft NPS server information:
  - RADIUS server Name (Any name example SE HQ NPS)
  - Up to three RADIUS IP addresses
  - RADIUS Authentication Port; default 1812/UDP
  - RADIUS Shared secret (pre-shared key that need to same NPS client pre-shard key)
  - Nile Geo scope (Site): Nile supports one RADIUS server per Geo scope.
- Click on DISPLAY NAS IP'S to get Nile Service Block NAS IP address that need to be added as Microsoft NPS client.



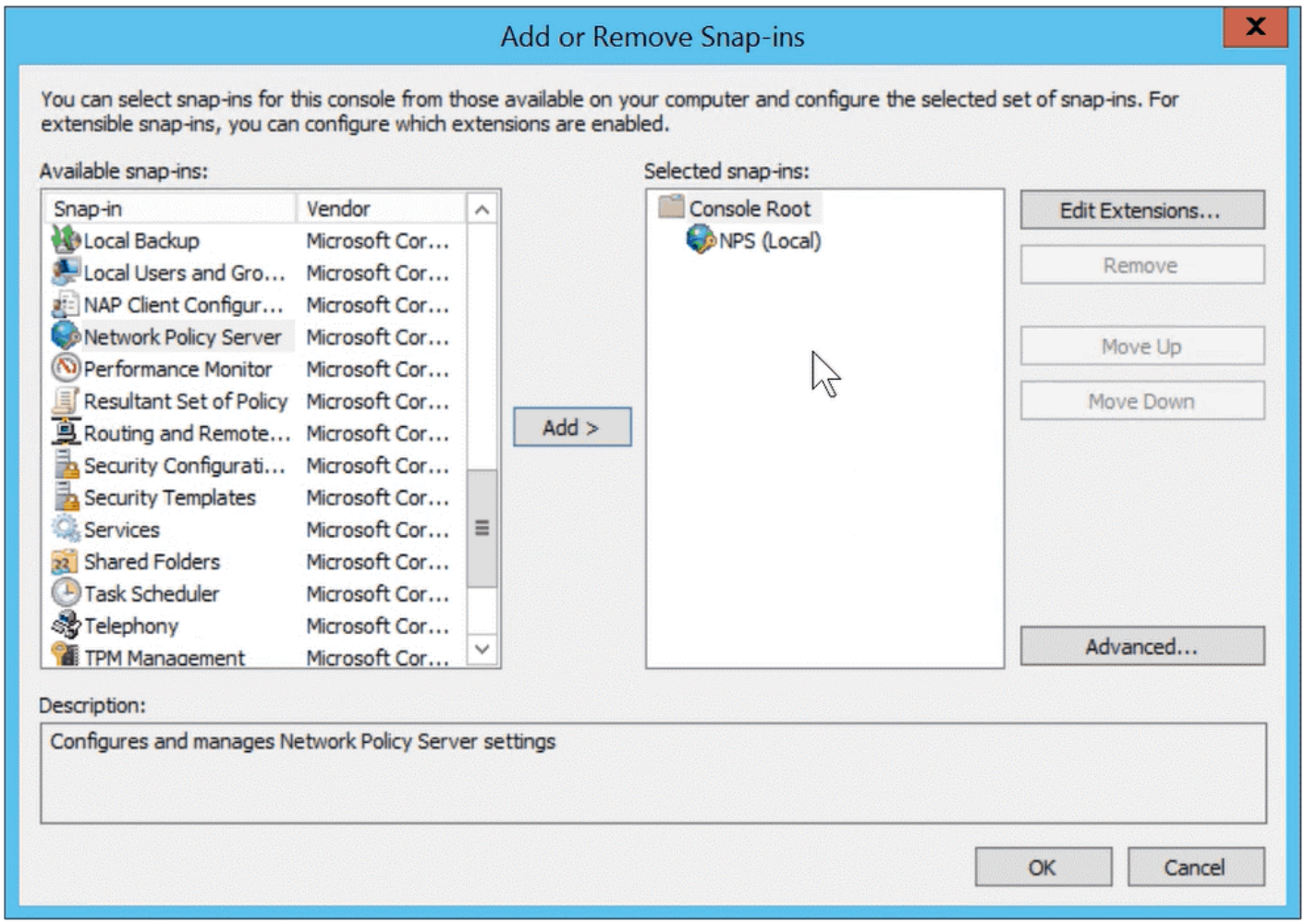
- The result is shown in the entry panel:



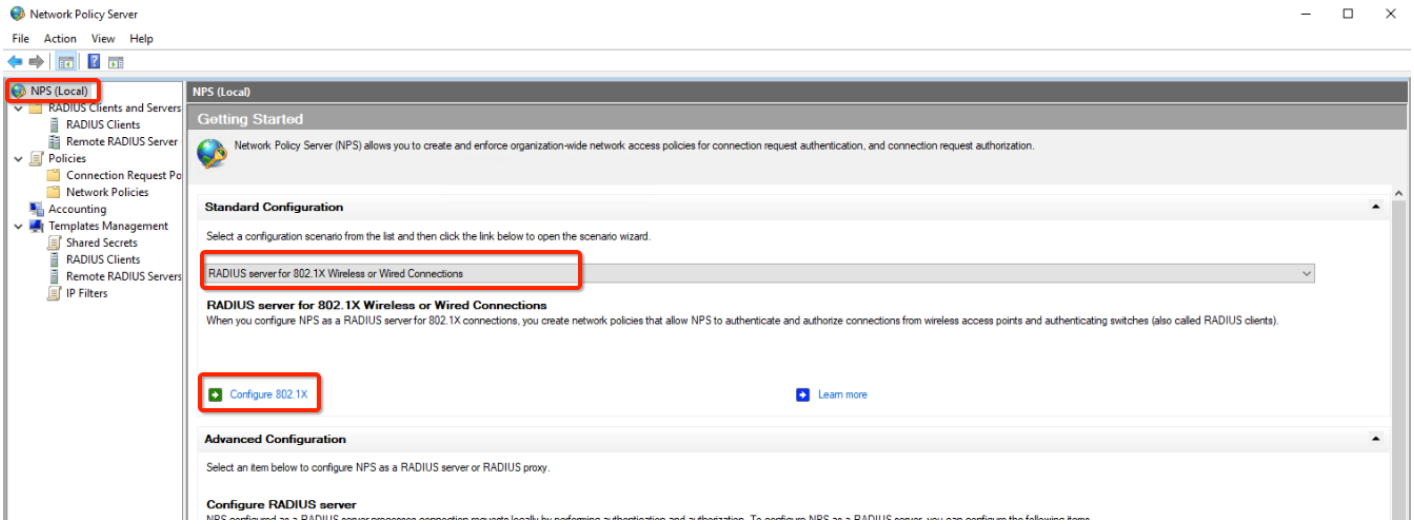
- Click on Save and verify the server added to the Authentication device list

Configuring NPS Server

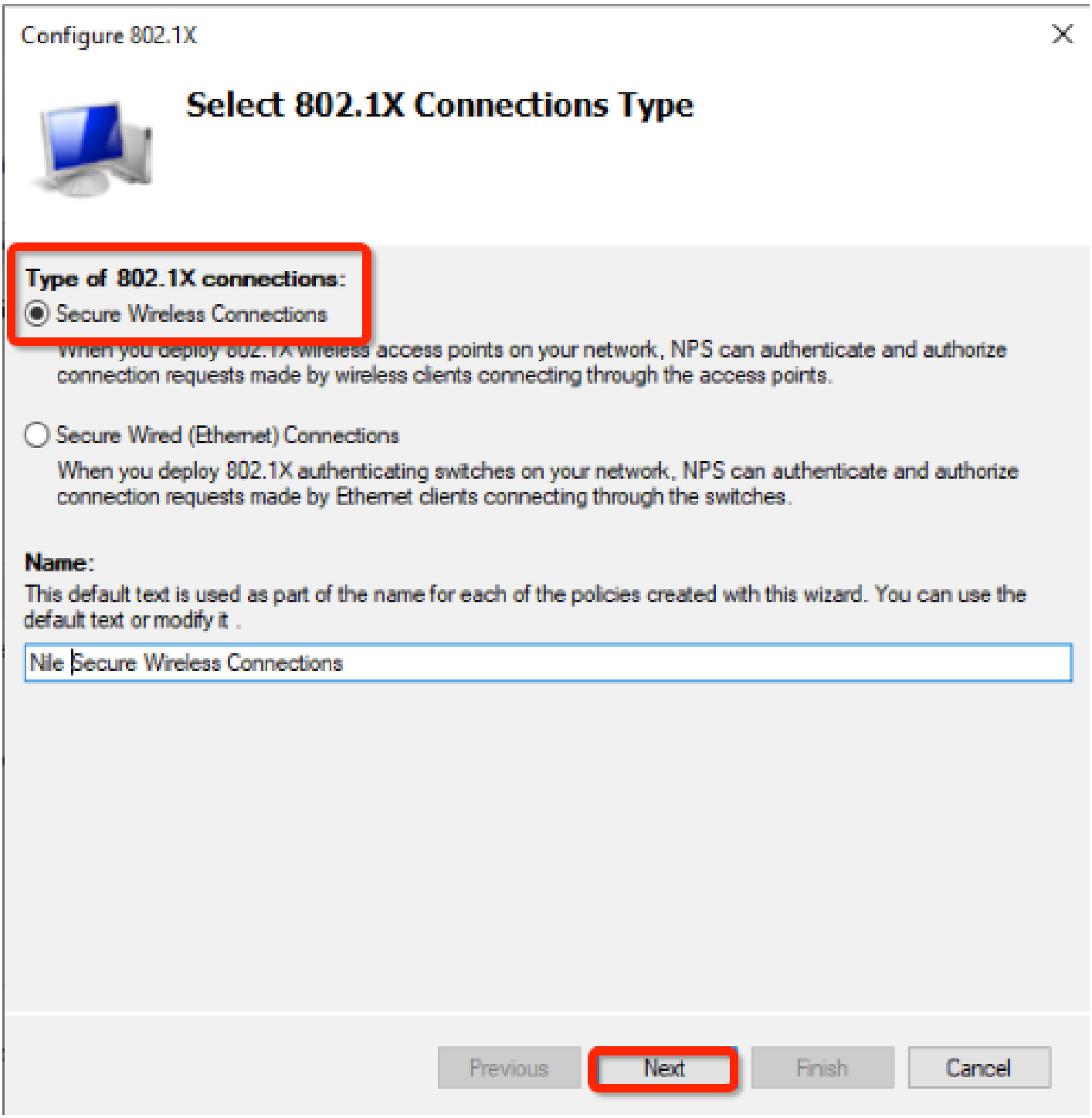
- Go to **Windows** ? **Run** ? **MMC**
- In the Console, navigate to **File** ? **Add/Remove Snap-in**
- In the Add/Remove Snap-in window, select **Network Policy Server**from the “Available snap-ins” window, and click the **Add** button
- In the **Select Computer** window, select “Local Computer”
- Click the **OK** button
- In the Add/Remove Snap-in window, click the **OK button**



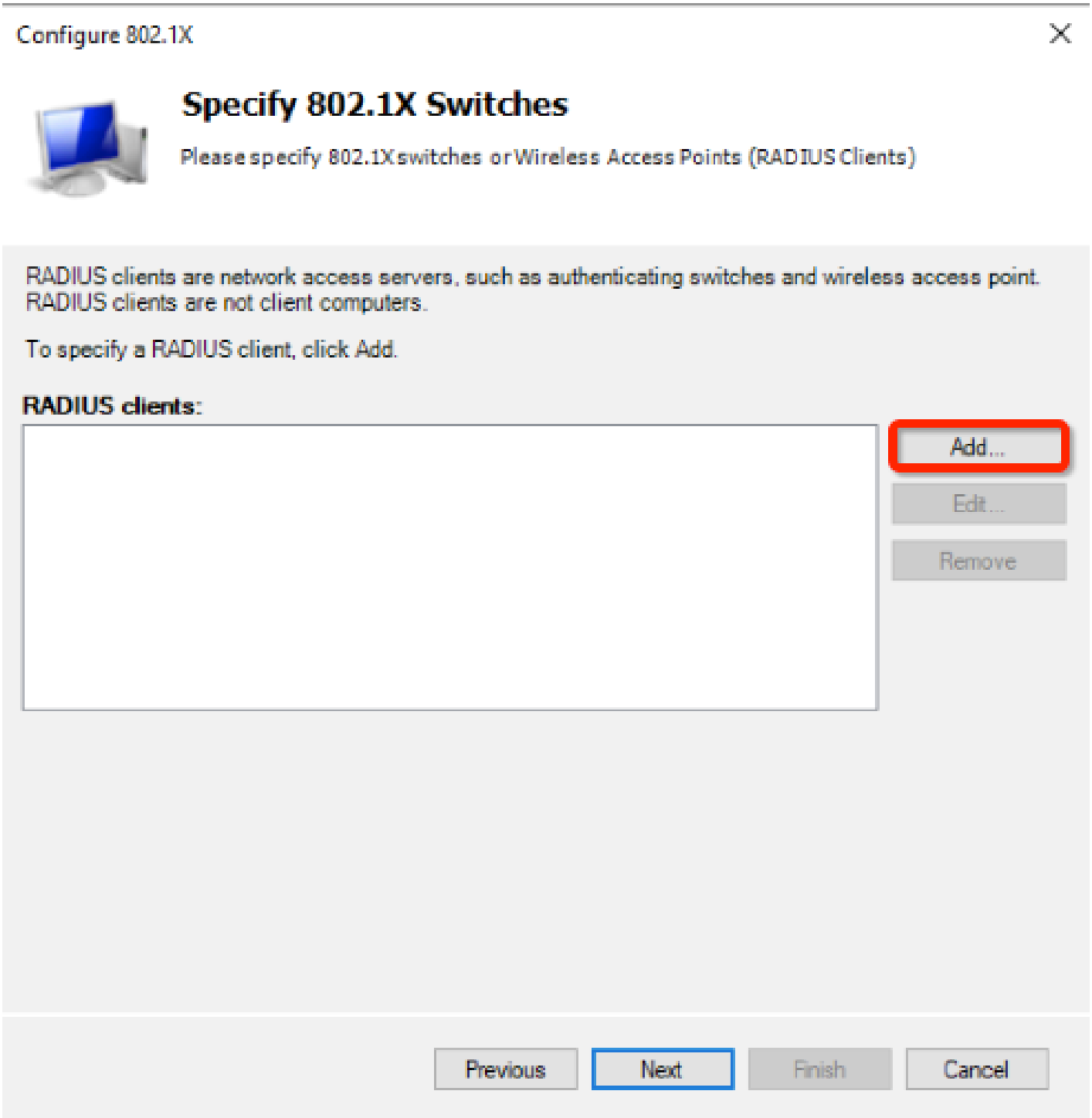
- In the Console, navigate to NPS (Local) side menu
- In the “Standard Configuration” panel, select “RADIUS server for 802.1x Wireless or Wired Connections” from the pull-down list
- Click on “+ Configure 8201.X” link: this launches the 802.1x configuration wizard.



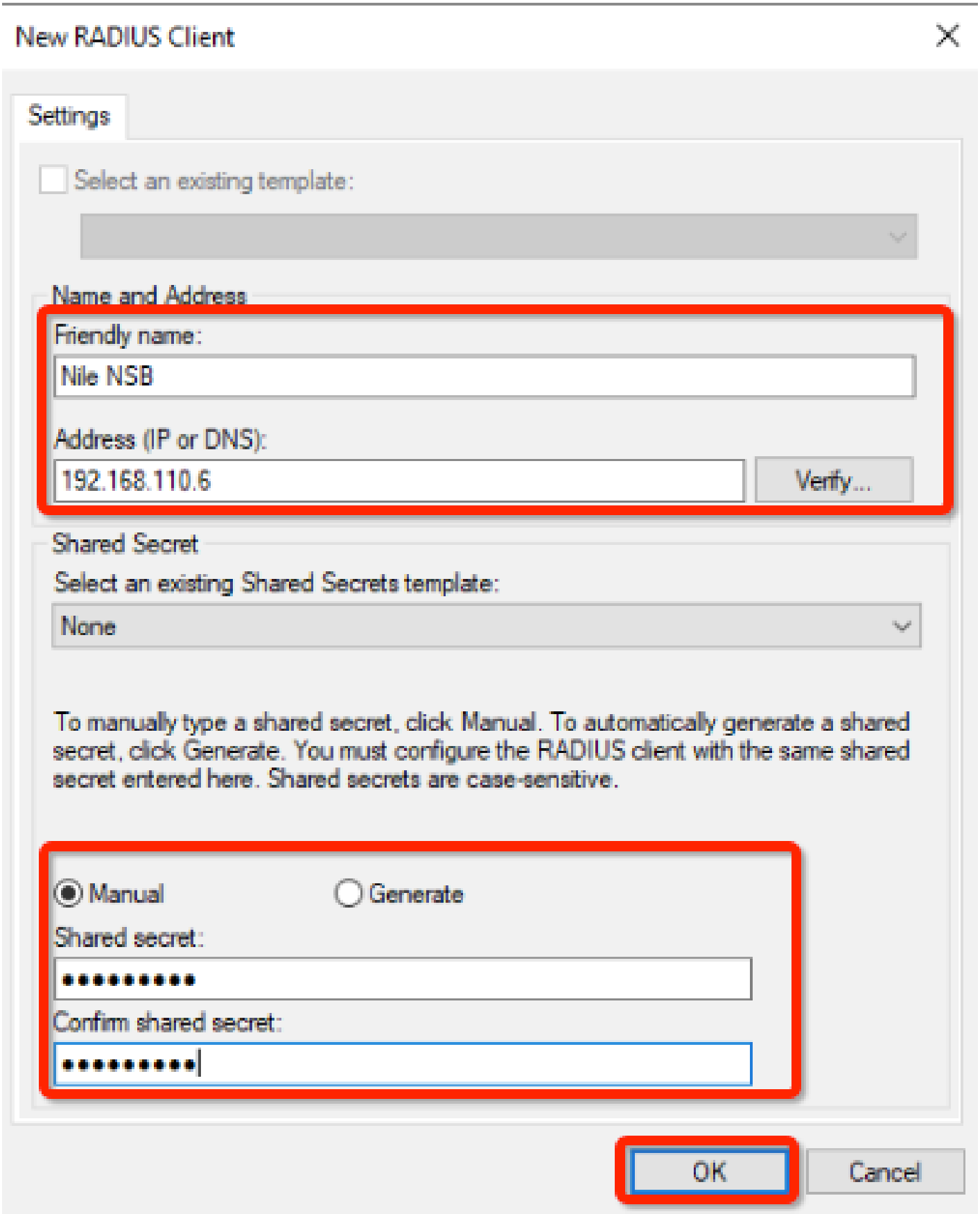
- Select **Secure Wireless Connections** radio button
- Add “Nile” to the beginning of the name
- Click the **Next** button



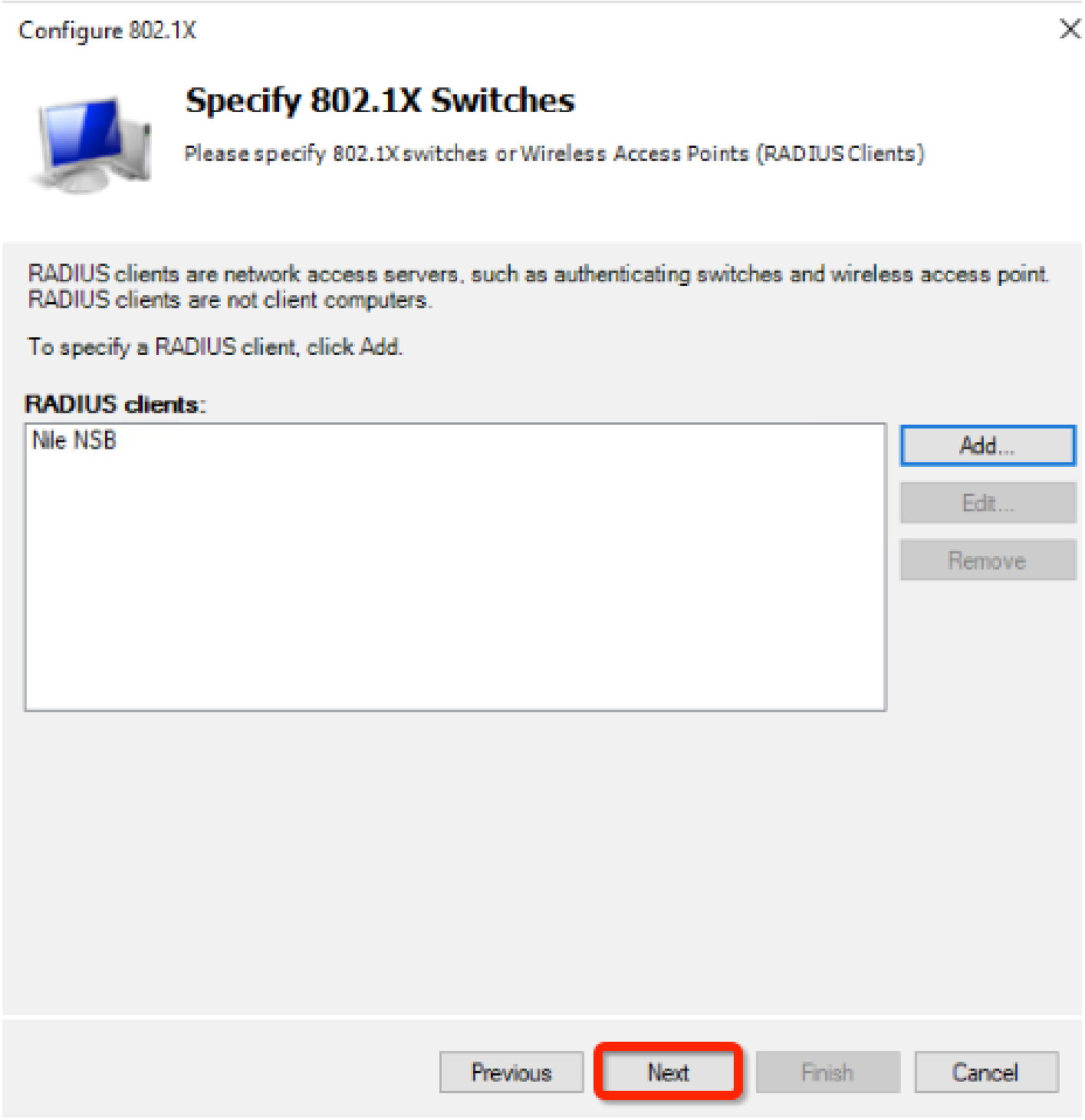
- Click the **Add…** button to add Nile RADIUS client



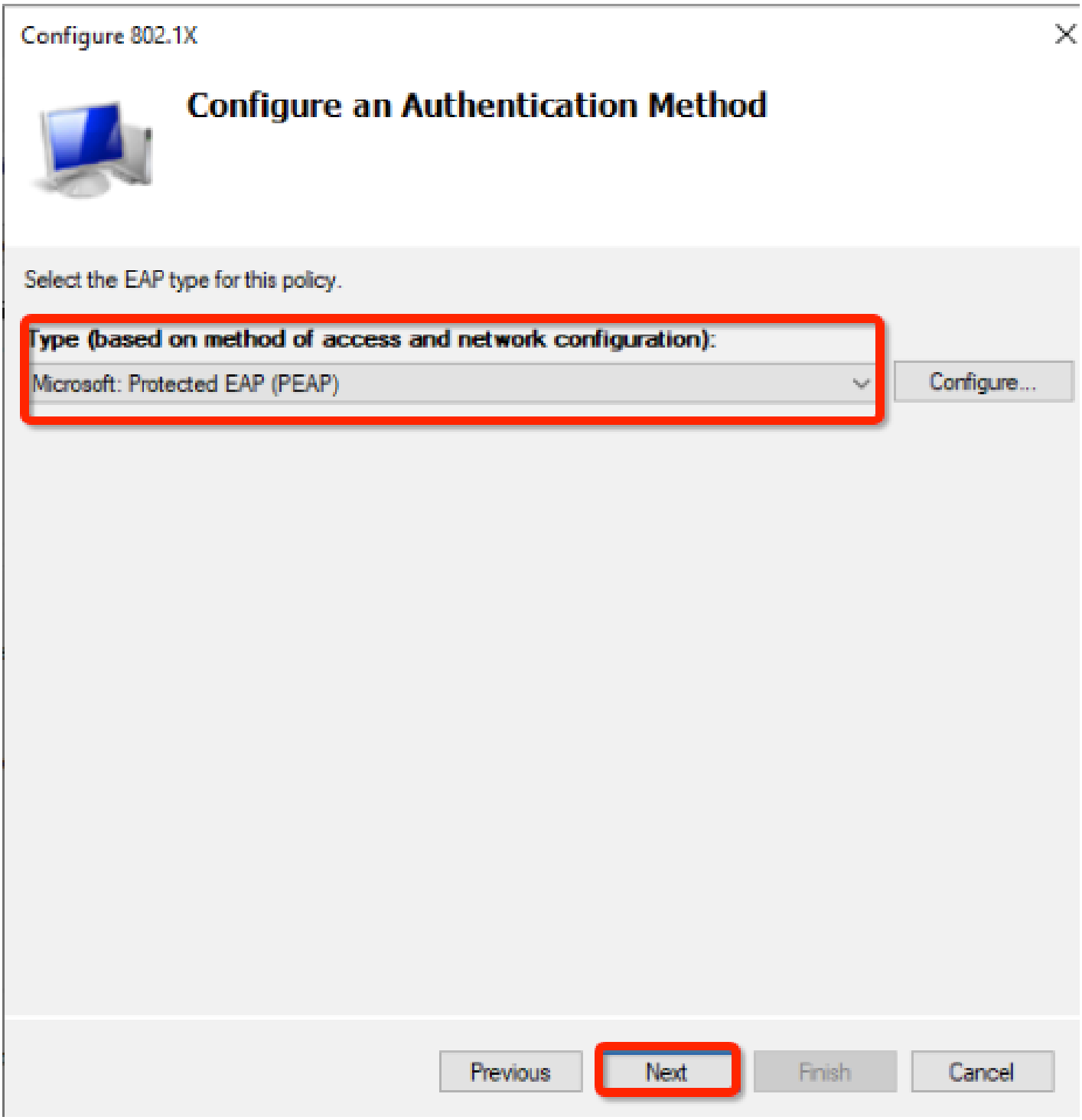
- Use “Nile NSB” as the Friendly name
- Fill in “Address (IP or DNS)” with the NAS IP address provided by the Nile Portal
- Click the **Manual** radio button
- Enter the secret that matches the one in the Nile Portal Authentication settings.
- Click on **OK** button



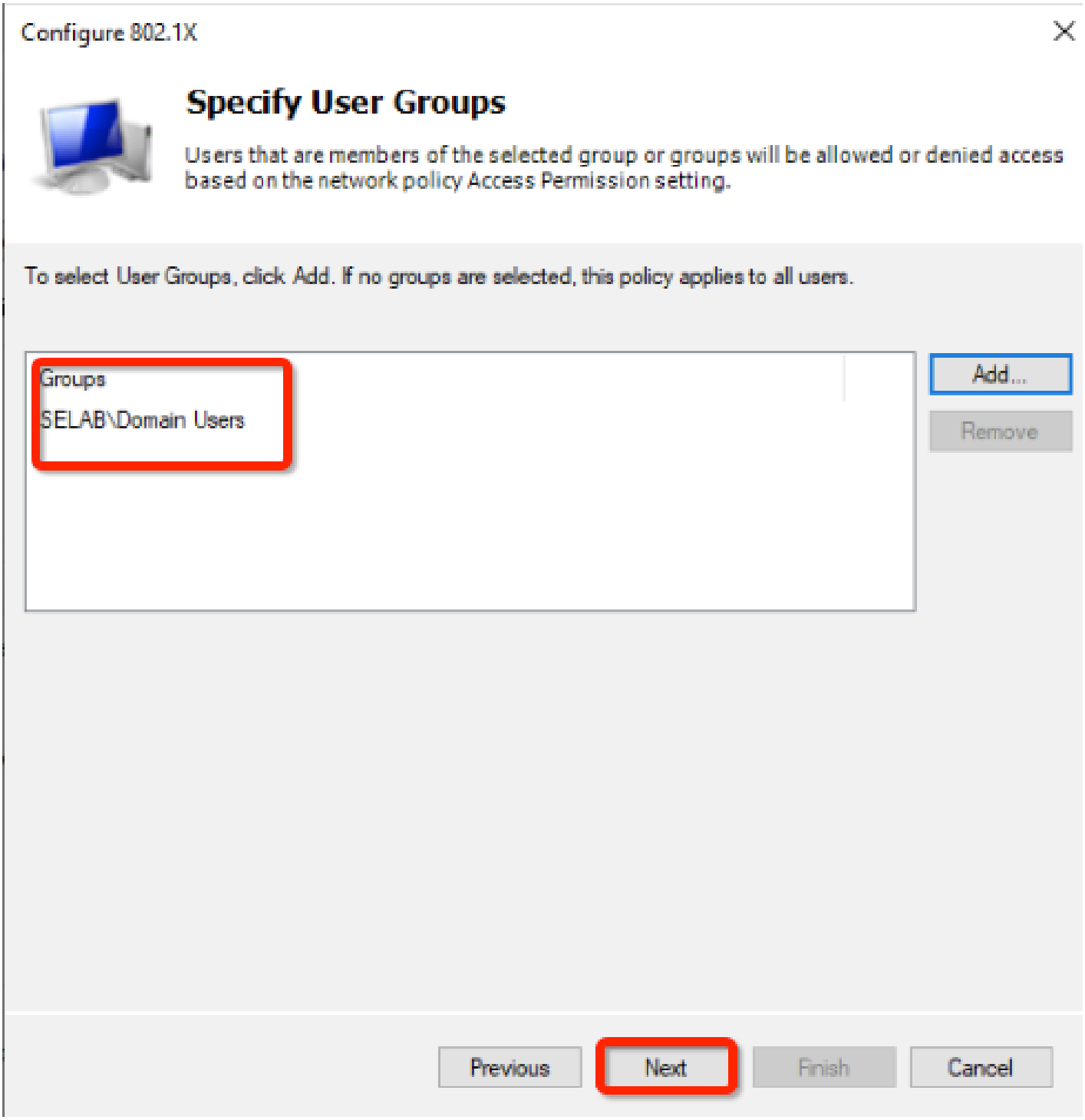
- This policy example allows only domain users;, to add these three conditions click the Next button



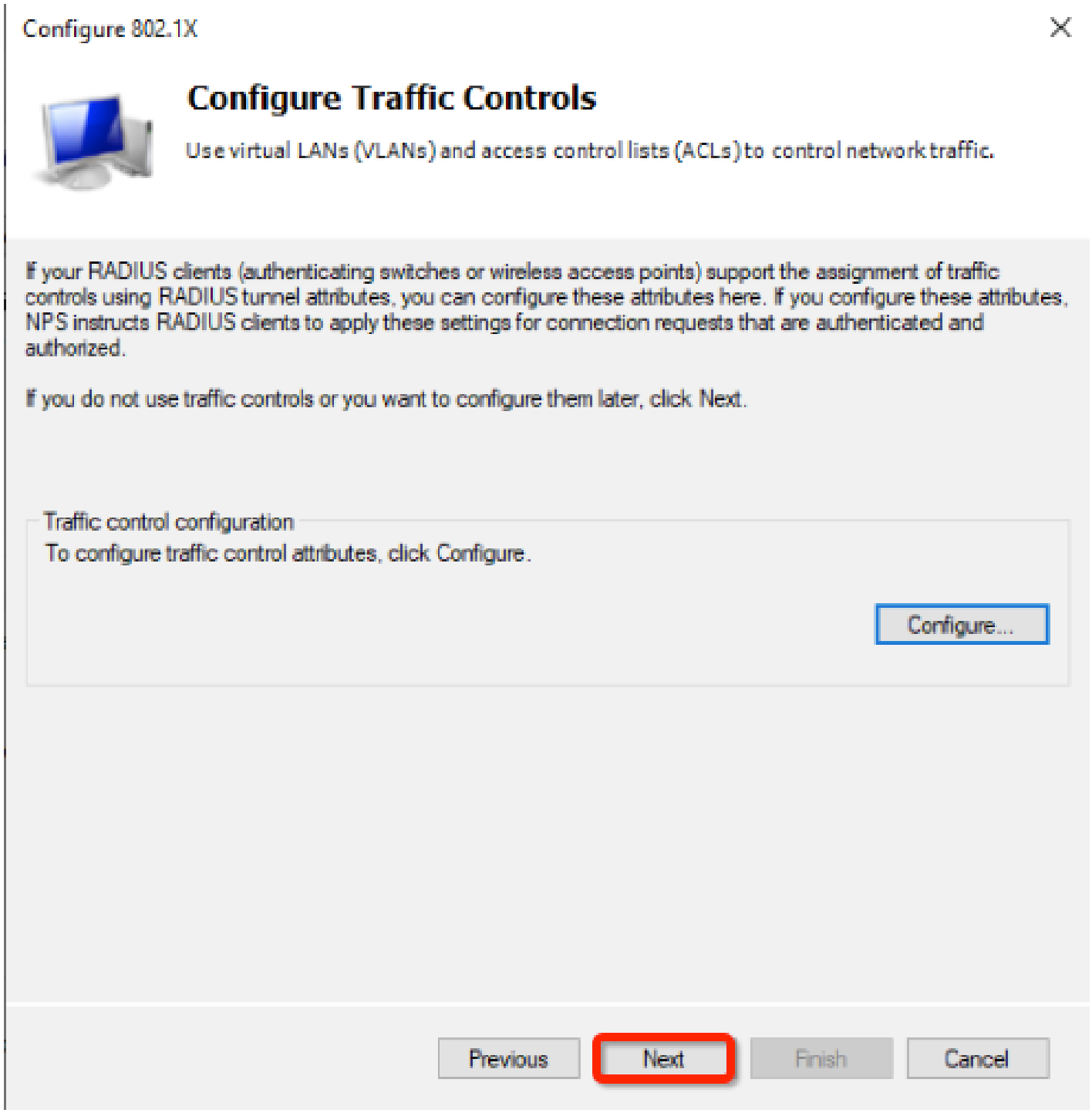
- Select Authentication Type – Microsoft: Protected EAP (PEAP) and click on Next



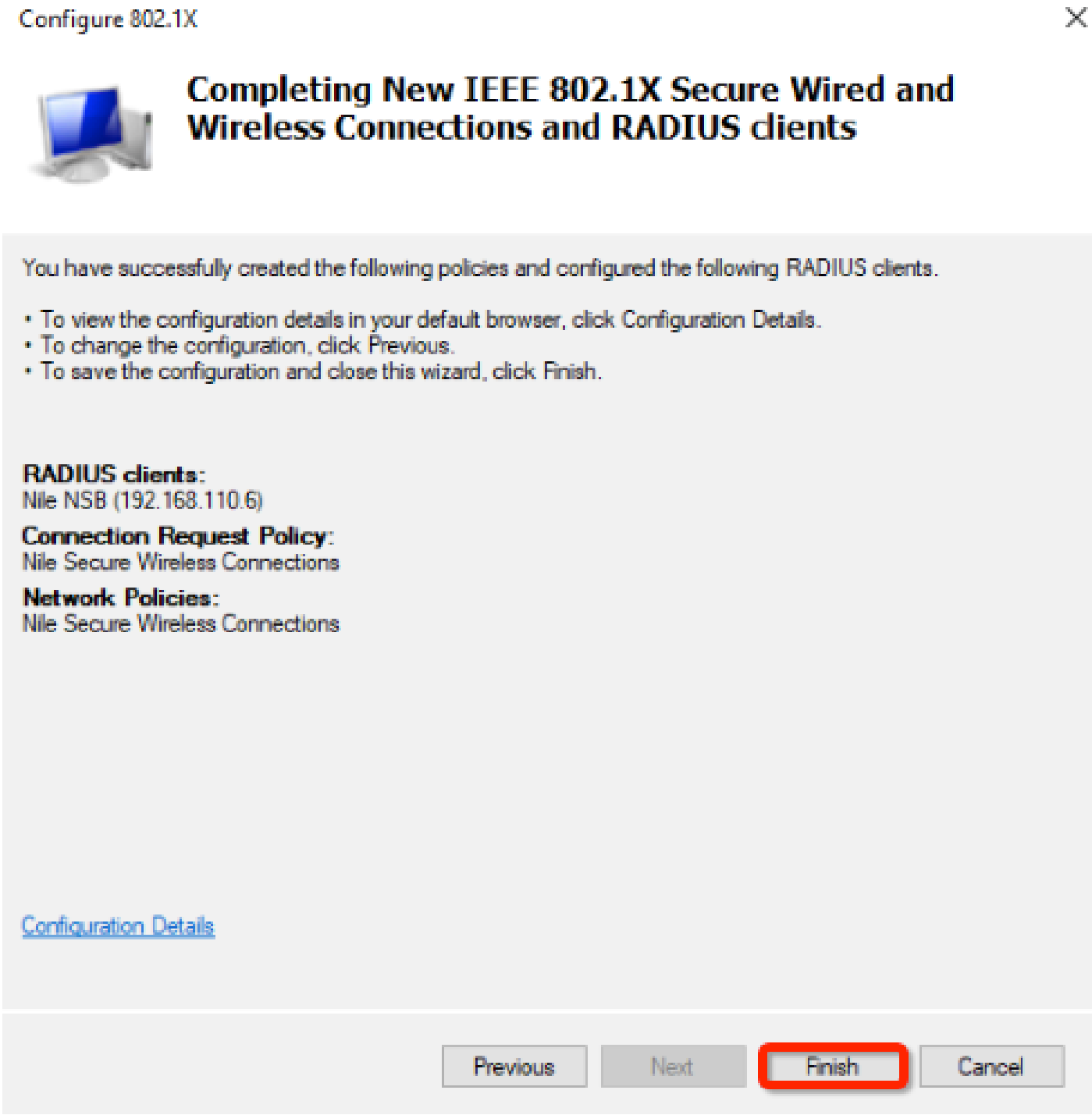
- Windows Groups – select user groups for the policy. In our example, we will select “Domain Users” groups. Then click on Next.



- For traffic controls, just click on the **Next** button to use default configurations.



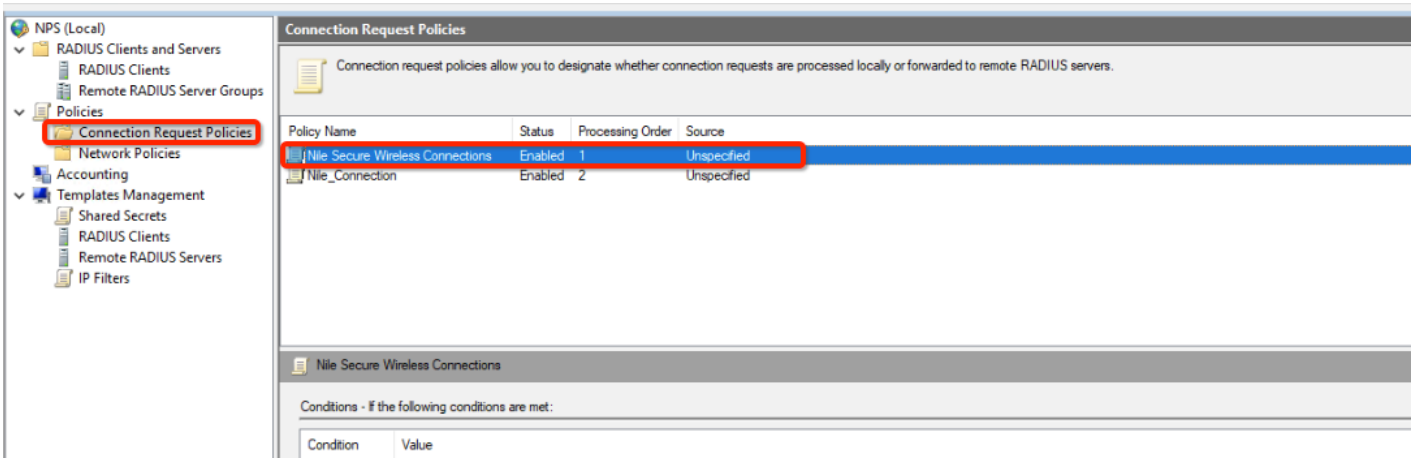
- Click on the **Finish** button to apply the setting.



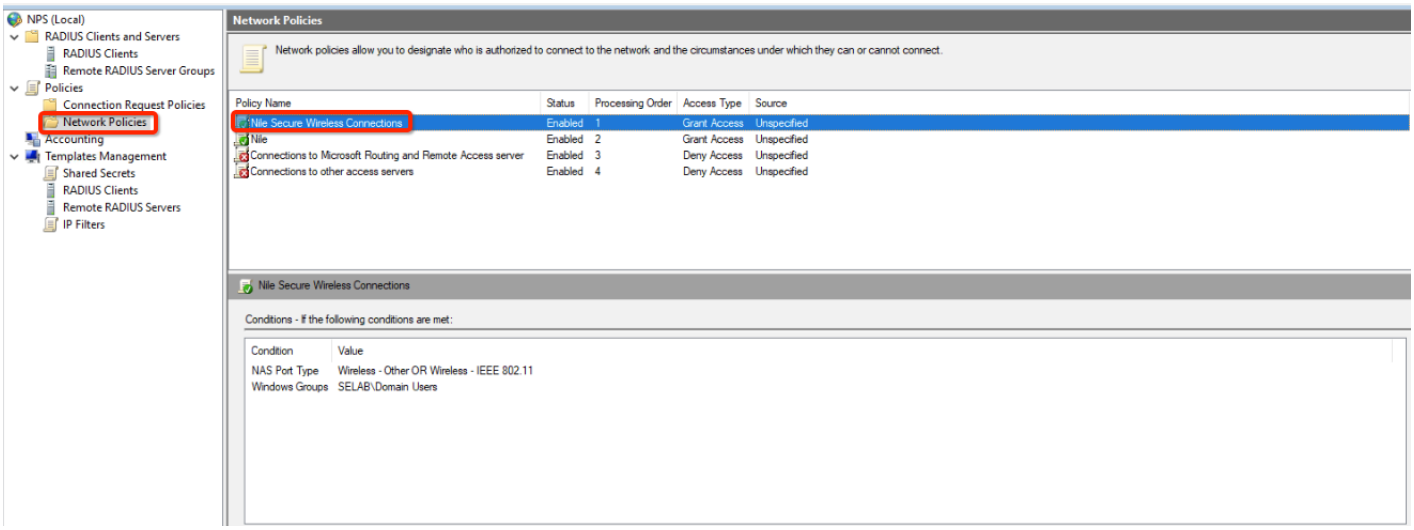
Note: This is just an example. You can modify the policy to meet your requirements.

For Machine Authentication or user authentication using a certificate, please select “Microsoft: Smart Card or other certificates.”

- In the left-hand menu, under “Policies” select “Connection Request Policies”
- Click the entry “Nile Secure Wireless Connections”.



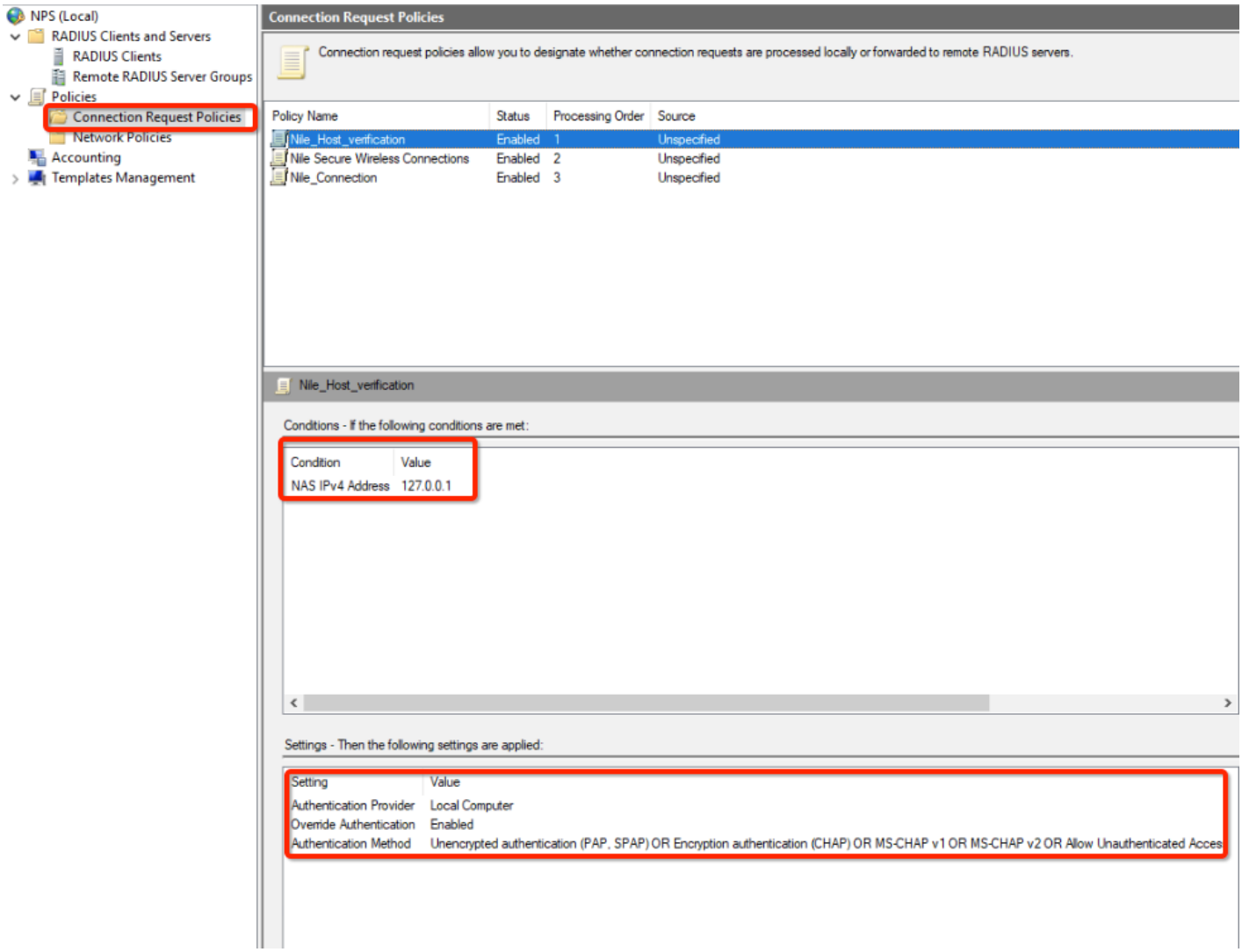
- In the left-hand menu, under “Policies”, select “Network Policies”.

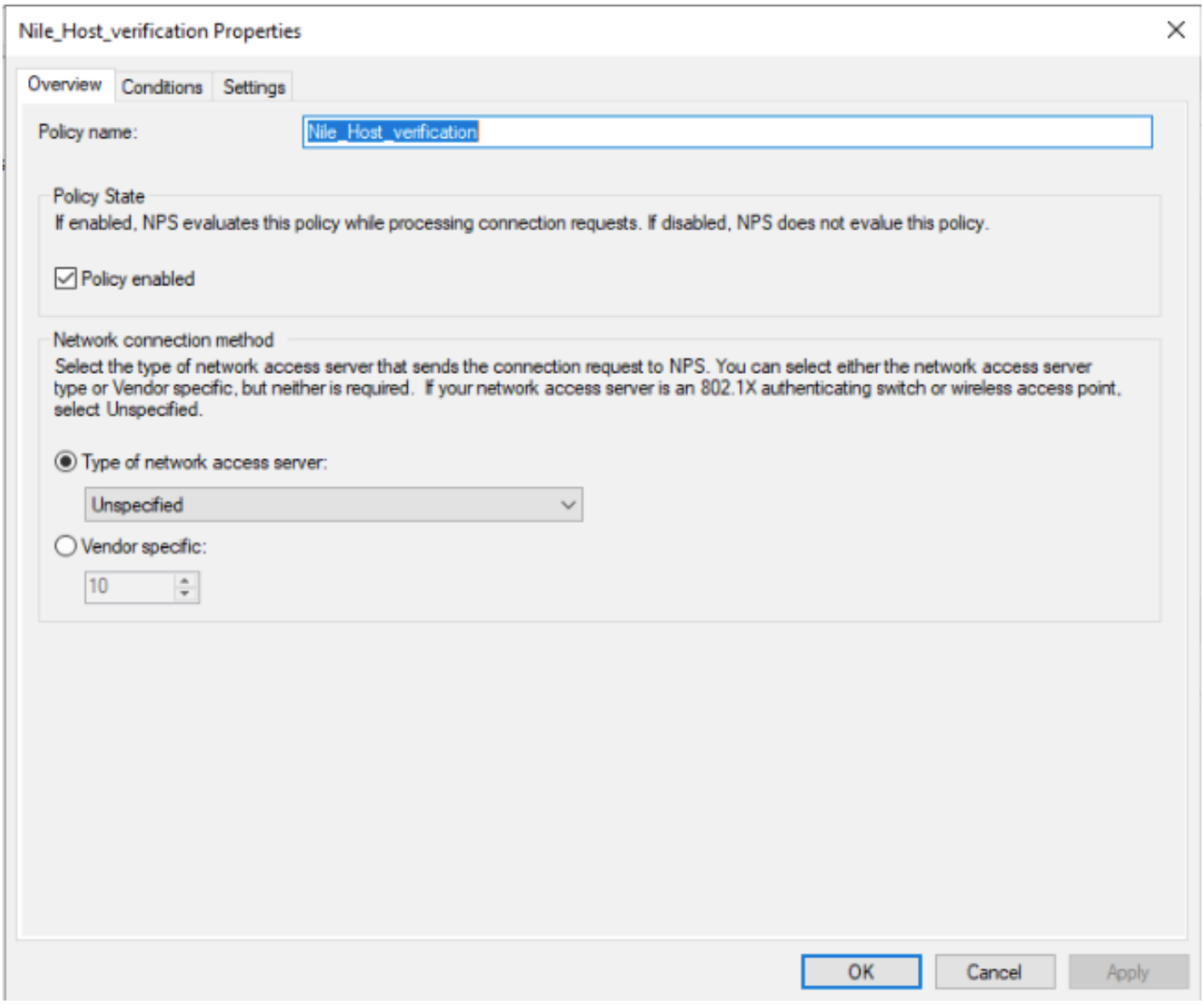


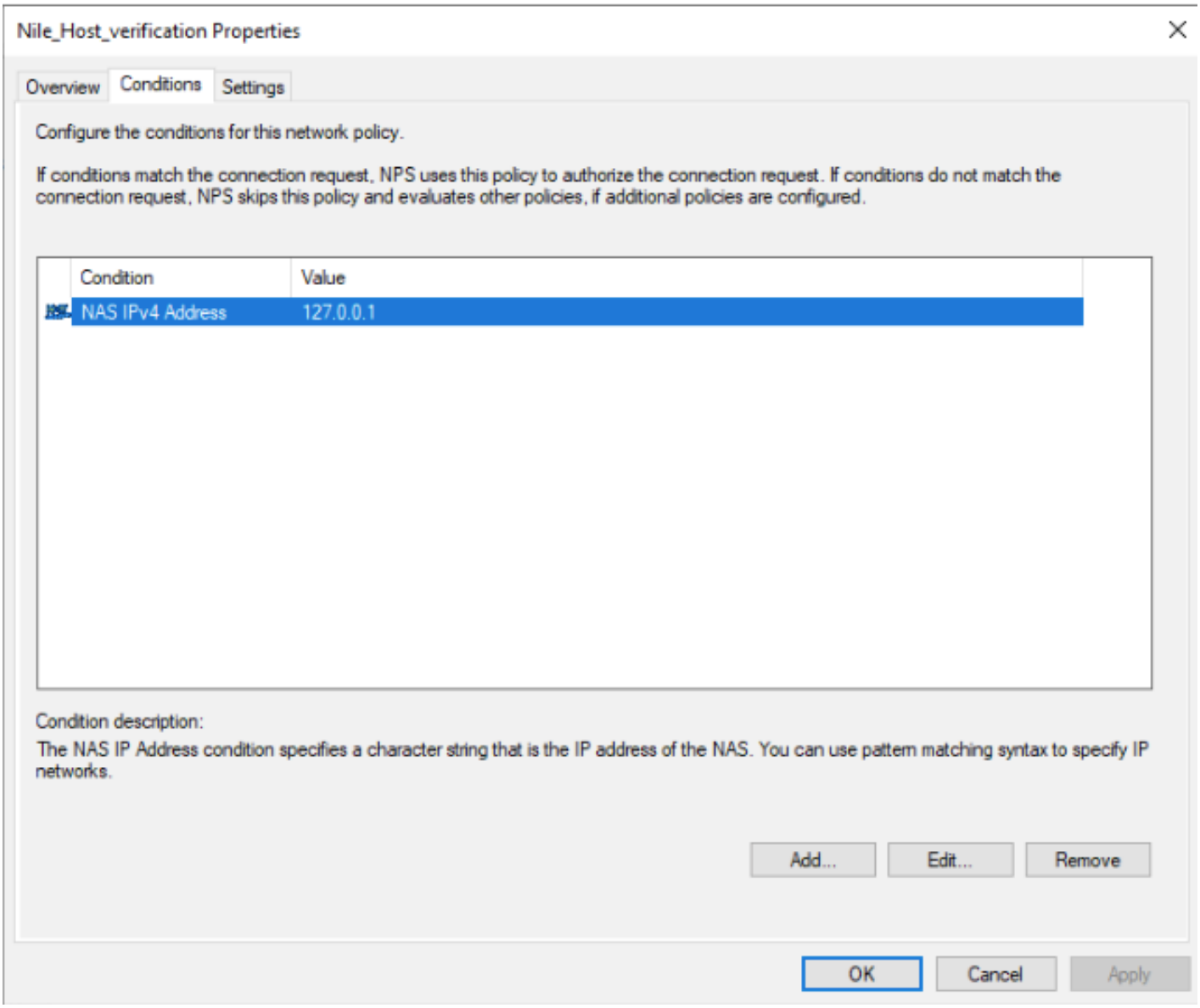
- Verify the information as shown.

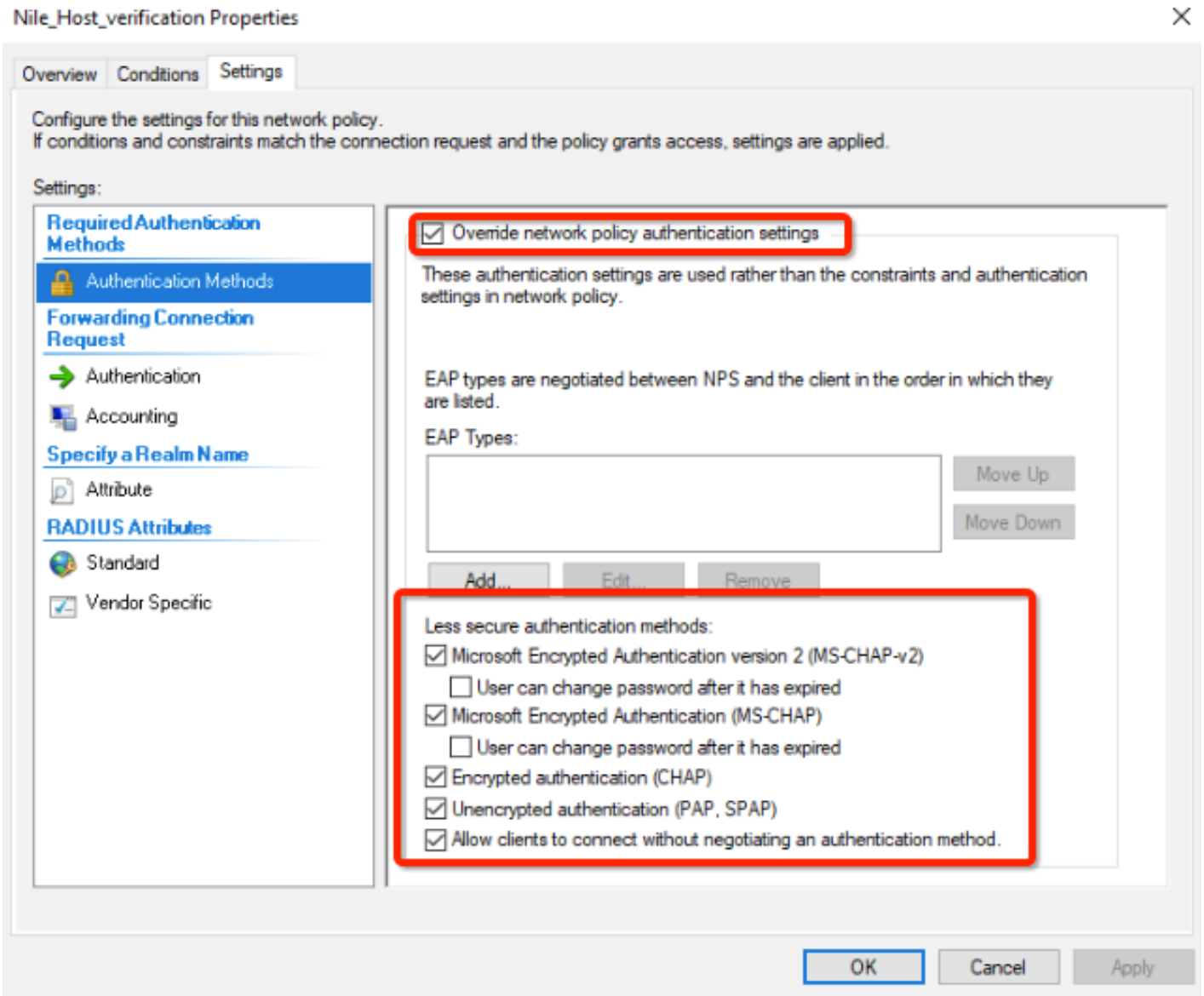
RADIUS Service Monitoring and Troubleshooting

- Nile supports RADIUS transaction monitoring for service availability, For monitoring, Nile will send an authentication request with a dummy user account “user name nile-network-test”, RADIUS will respond with a rejection which confirms RADIUS service is available.
- An administrator has the option to use an active directory user for monitoring or can run a one-time verification for troubleshooting only, Nile supports MS-CHAPv2 for RADIUS monitoring and requires an NPS policy for verification.
  Example: to allow Nile account verification, we need to have an NPS policy that allows MS-CHAP for local NPS (127.0.0.1)
- Create a new connection request policy name Nile_Host_Verifcation

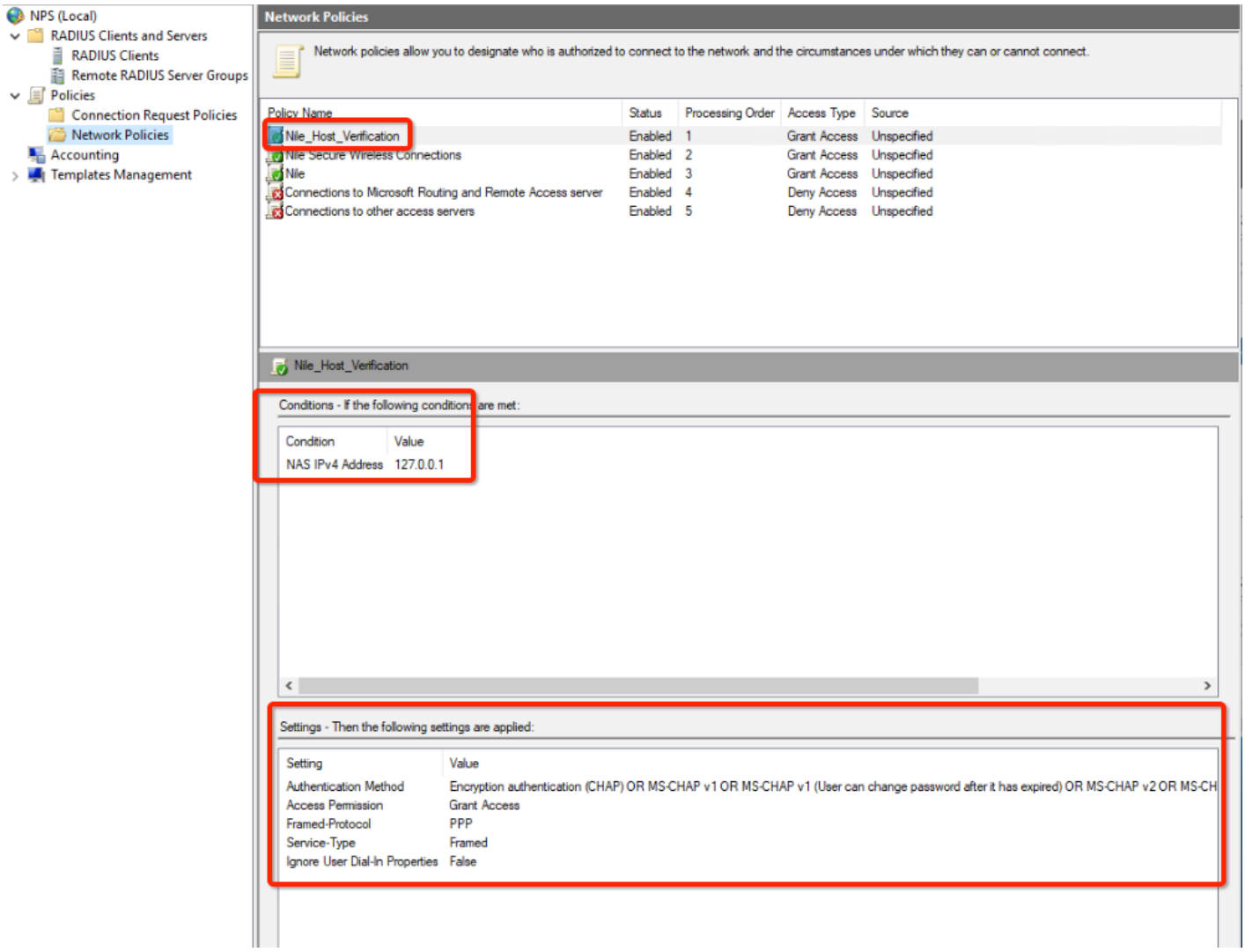

NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Accounting
Templates Management
Connection Request Policies
Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.
Policy Name
Status
Processing Order
Source
Nile_Host_verification
Enabled
1
Unspecified
Nile Secure Wireless Connections
Enabled
2
Unspecified
Nile_Connection
Enabled
3
Unspecified
Nile_Host_verification
Conditions - If the following conditions are met:
Condition
Value
NAS IPv4 Address
127.0.0.1
Settings - Then the following settings are applied:
Setting
Value
Authentication Provider
Local Computer
Override Authentication
Enabled
Authentication Method
Unencrypted authentication (PAP, SPAP) OR Encryption authentication (CHAP) OR MS-CHAP v1 OR MS-CHAP v2 OR Allow Unauthenticated Acces

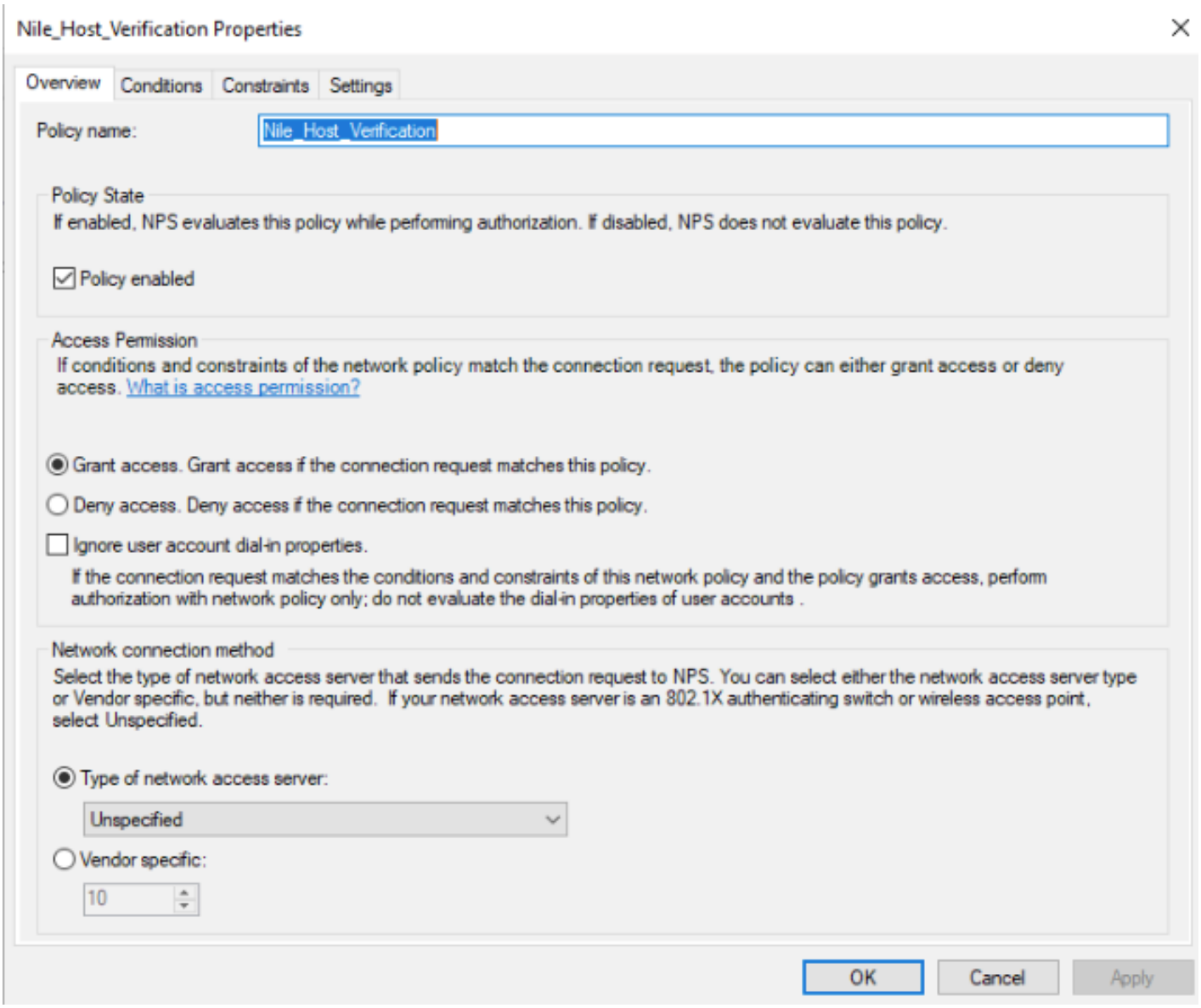

Nile_Host_verification Properties
Overview
Conditions
Settings
Policy name:
Nile_Host_verification
Policy State
If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy.
Policy enabled
Network connection method
Select the type of network 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
OK
Cancel
Apply

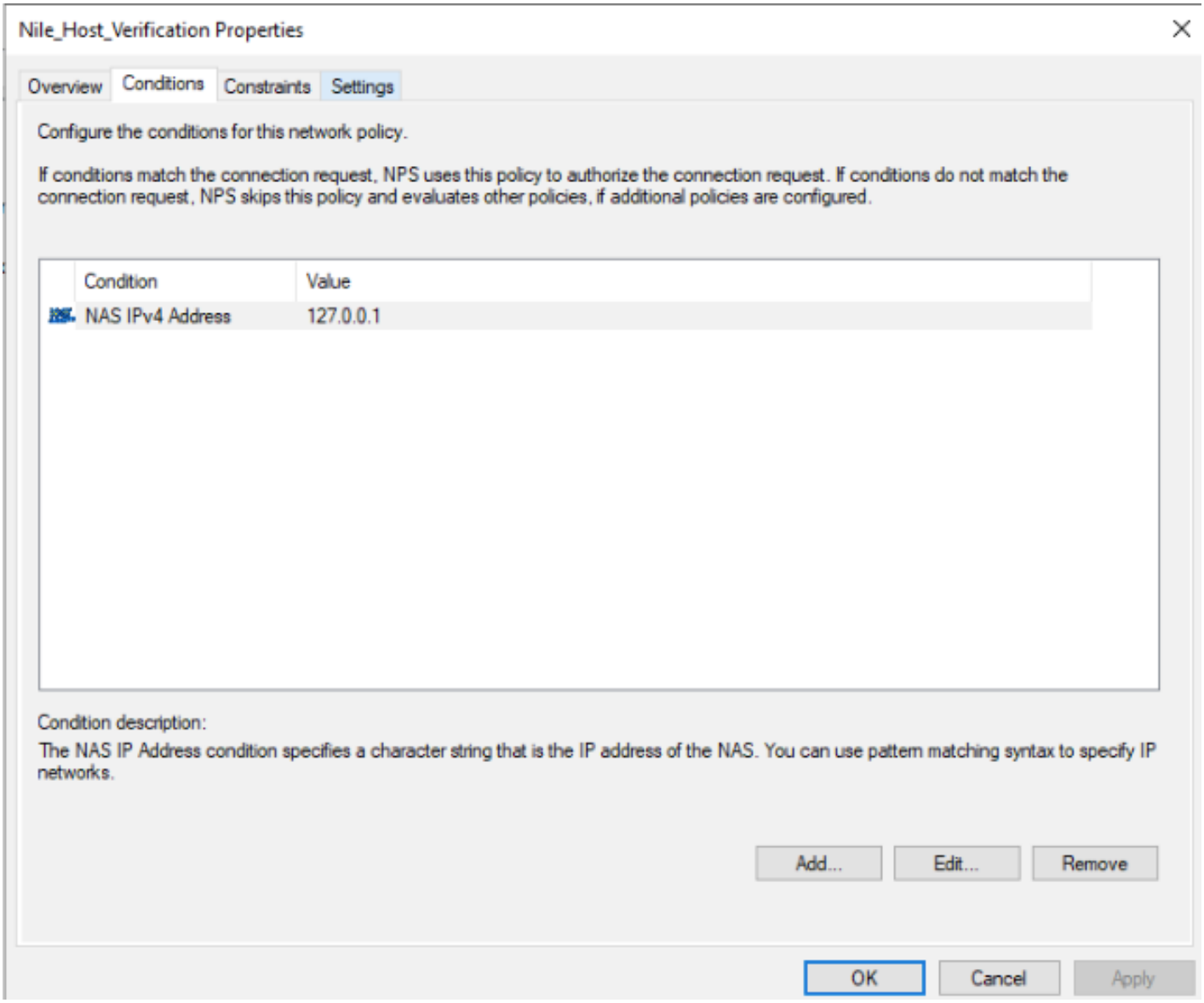

Nile_Host_verification Properties
Overview
Conditions
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
NAS IPv4 Address
127.0.0.1
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
OK
Cancel
Apply

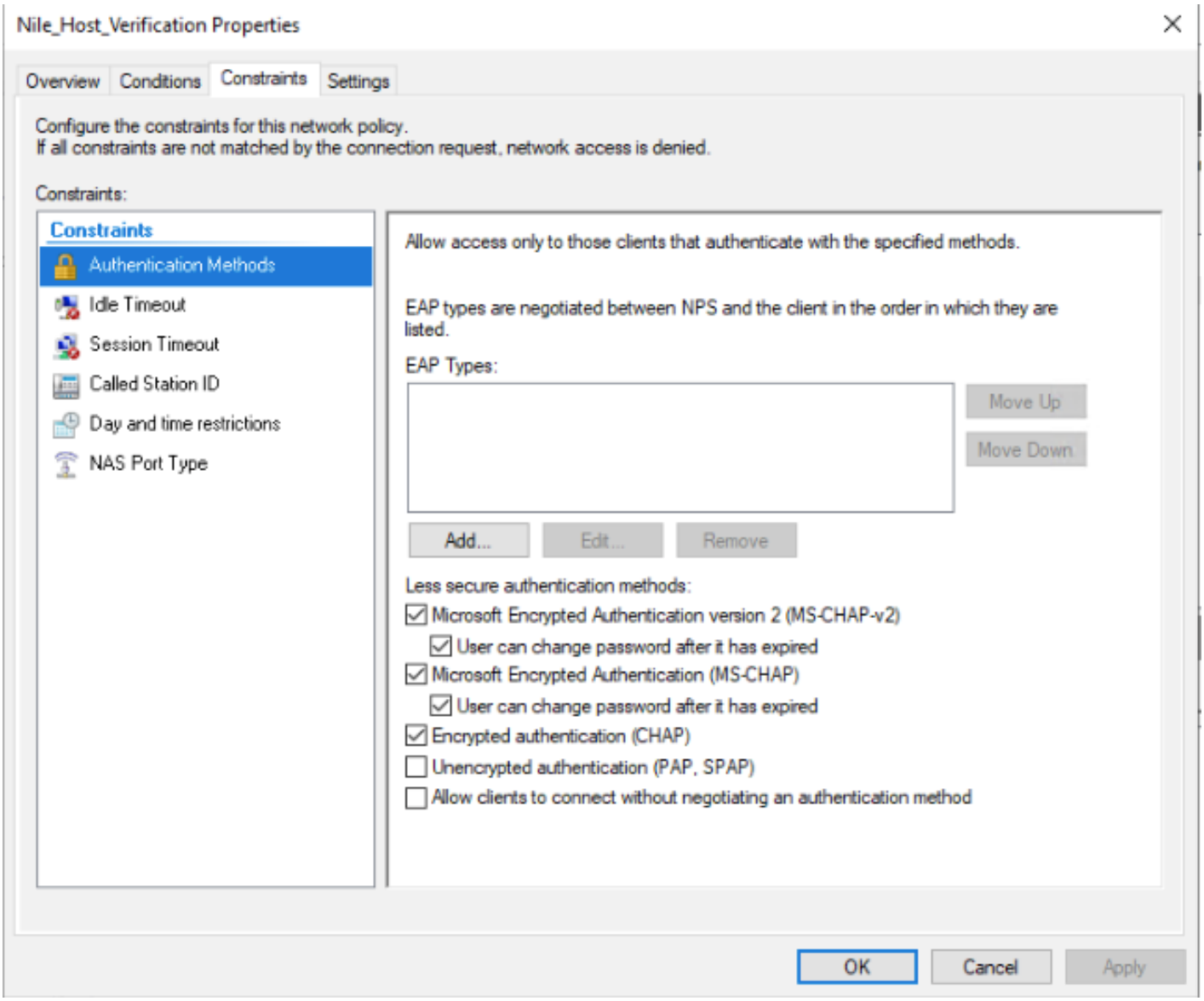


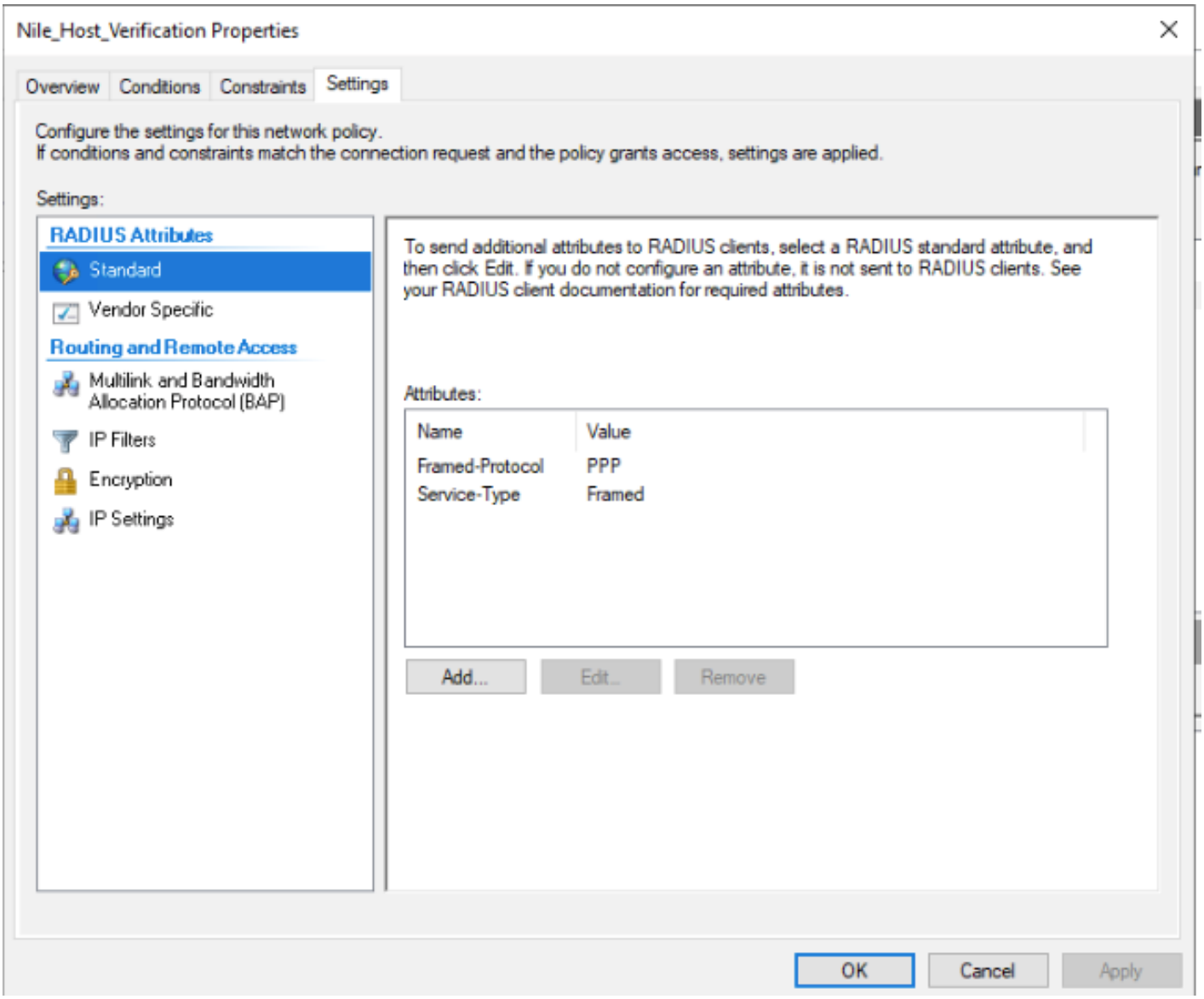
- Create a new Network policy name Nile_Host_Verifcation


NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Accounting
Templates Management
Network Policies
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
Policy Name
Status
Processing Order
Access Type
Source
Nile_Host_Verification
Enabled
1
Grant Access
Unspecified
Nile Secure Wireless Connections
Enabled
2
Grant Access
Unspecified
Nile
Enabled
3
Grant Access
Unspecified
Connections to Microsoft Routing and Remote Access server
Enabled
4
Deny Access
Unspecified
Connections to other access servers
Enabled
5
Deny Access
Unspecified
Nile_Host_Verification
Conditions - If the following conditions are met:
Condition
Value
NAS IPv4 Address
127.0.0.1
Settings - Then the following settings are applied:
Setting
Value
Authentication Method
Encryption authentication (CHAP) OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 OR MS-CH
Access Permission
Grant Access
Framed-Protocol
PPP
Service-Type
Framed
Ignore User Dial-In Properties
False


Nile_Host_Verification Properties
Overview
Conditions
Constraints
Settings
Policy name:
Nile_Host_Verification
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:
Unspecified
Vendor specific:
10
OK
Cancel
Apply

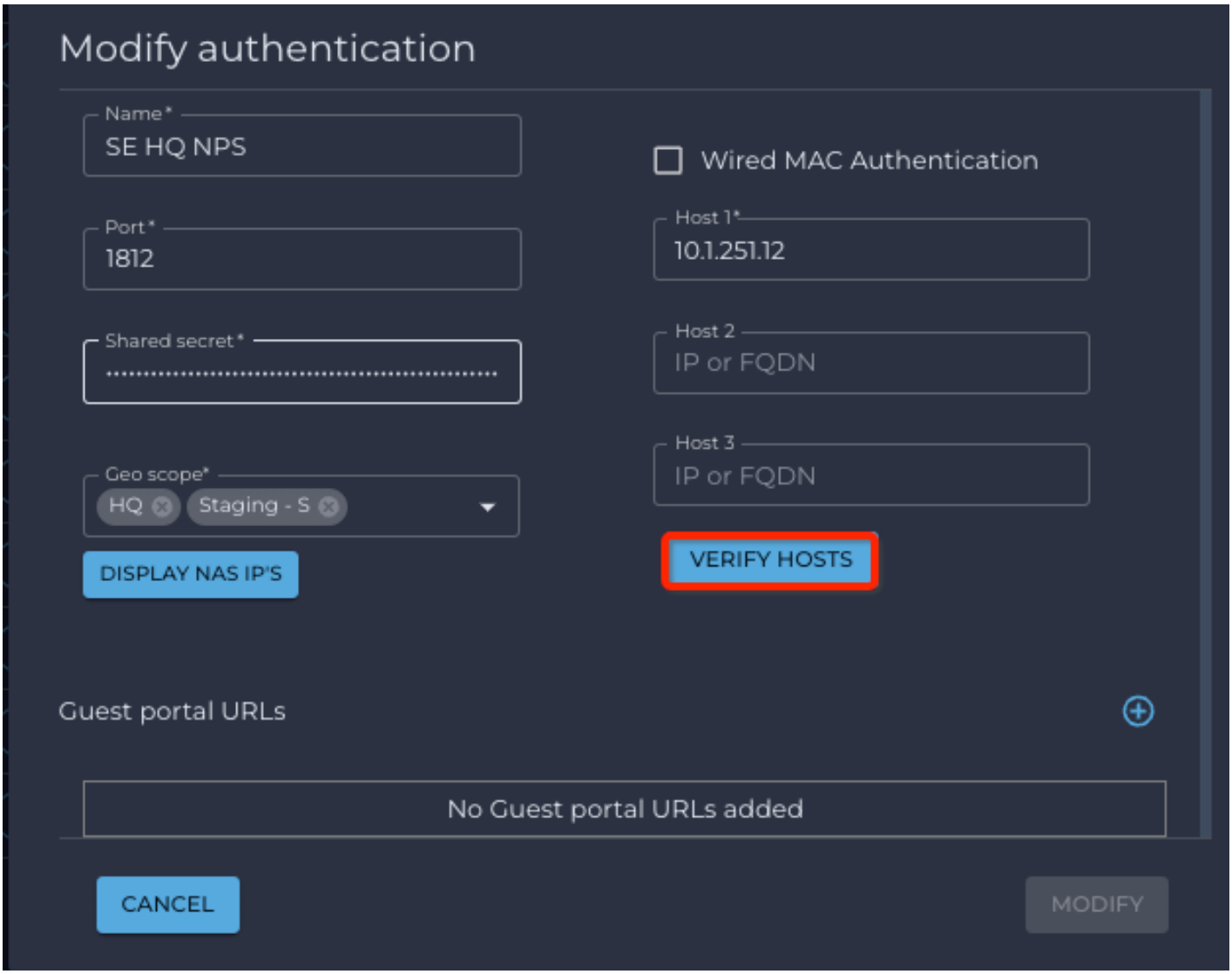

Nile_Host_Verification Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
NAS IPv4 Address
127.0.0.1
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
OK
Cancel
Apply


Nile_Host_Verification Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only to those clients that authenticate with the specified methods.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Move Up
Move Down
Add...
Edit...
Remove
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
OK
Cancel
Apply

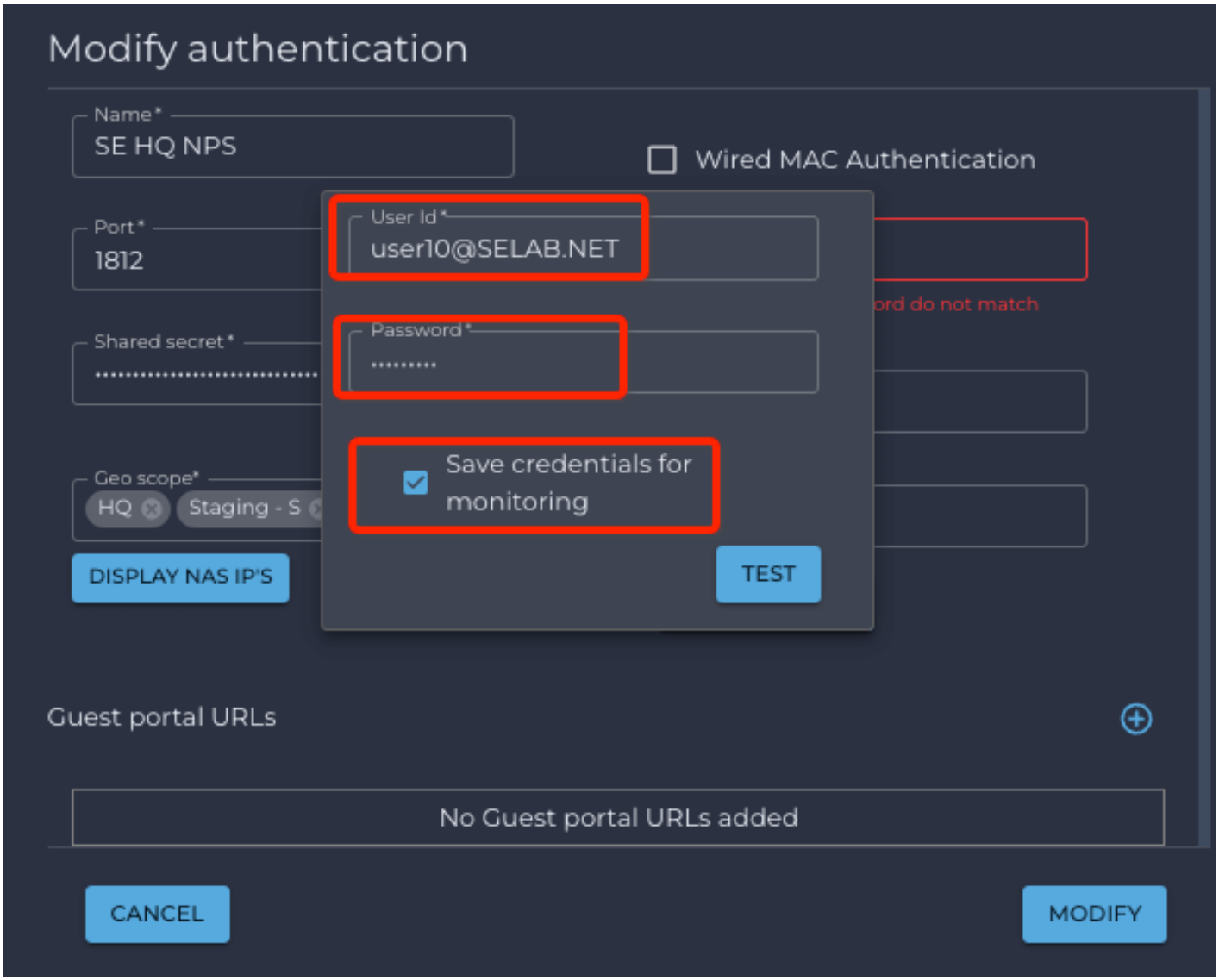


- To verify RADIUS authentication, log onto Nile Portal: https://u1.nile-global.cloud/
- Navigate to **Nile Portal ® Settings** button ® **Authentication** tab
- Click on the blue RADIUS hostname (Example SE HQ NPS)

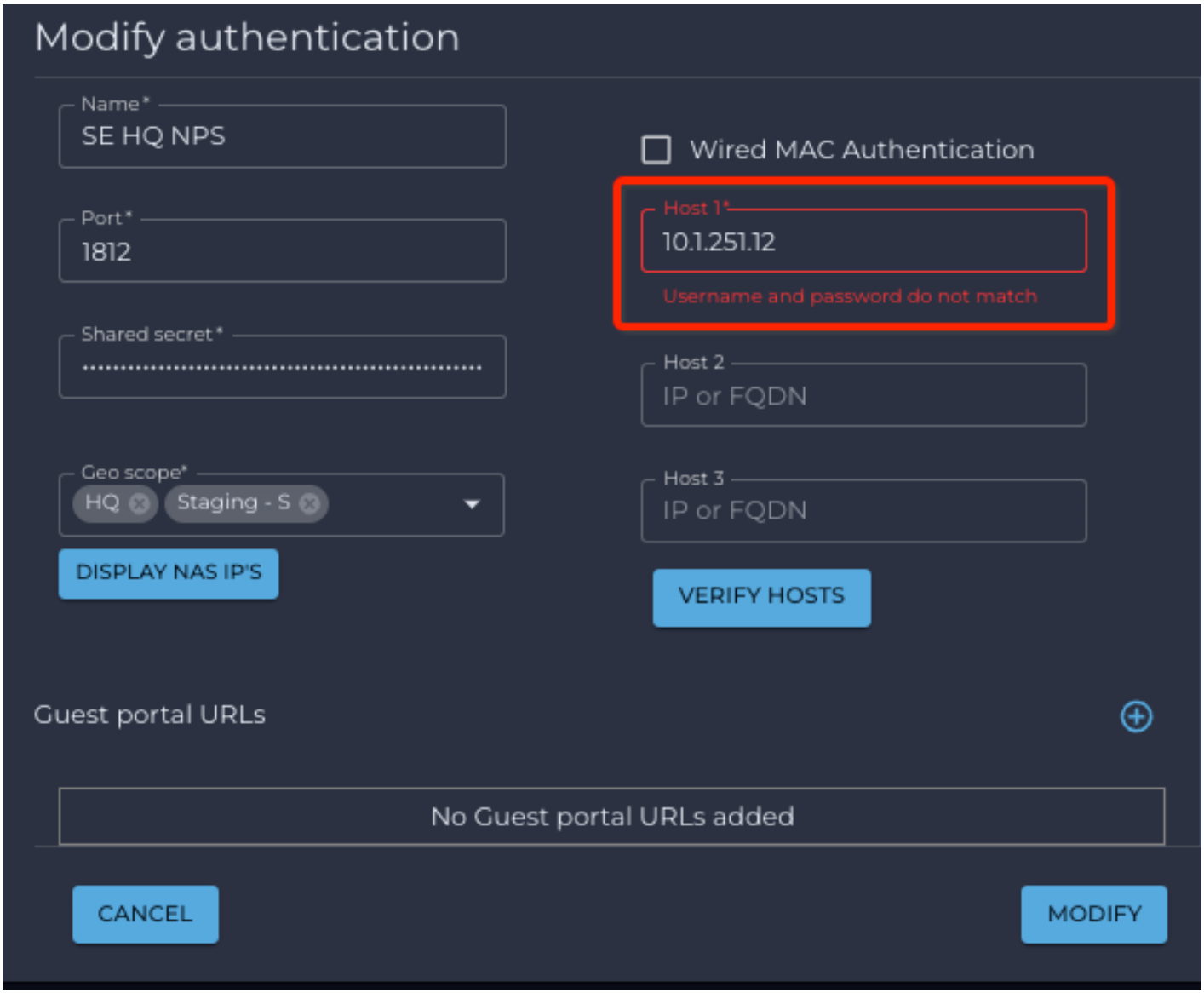
- From RADIUS configuration modification page, click on **VERIFY HOSTS** button



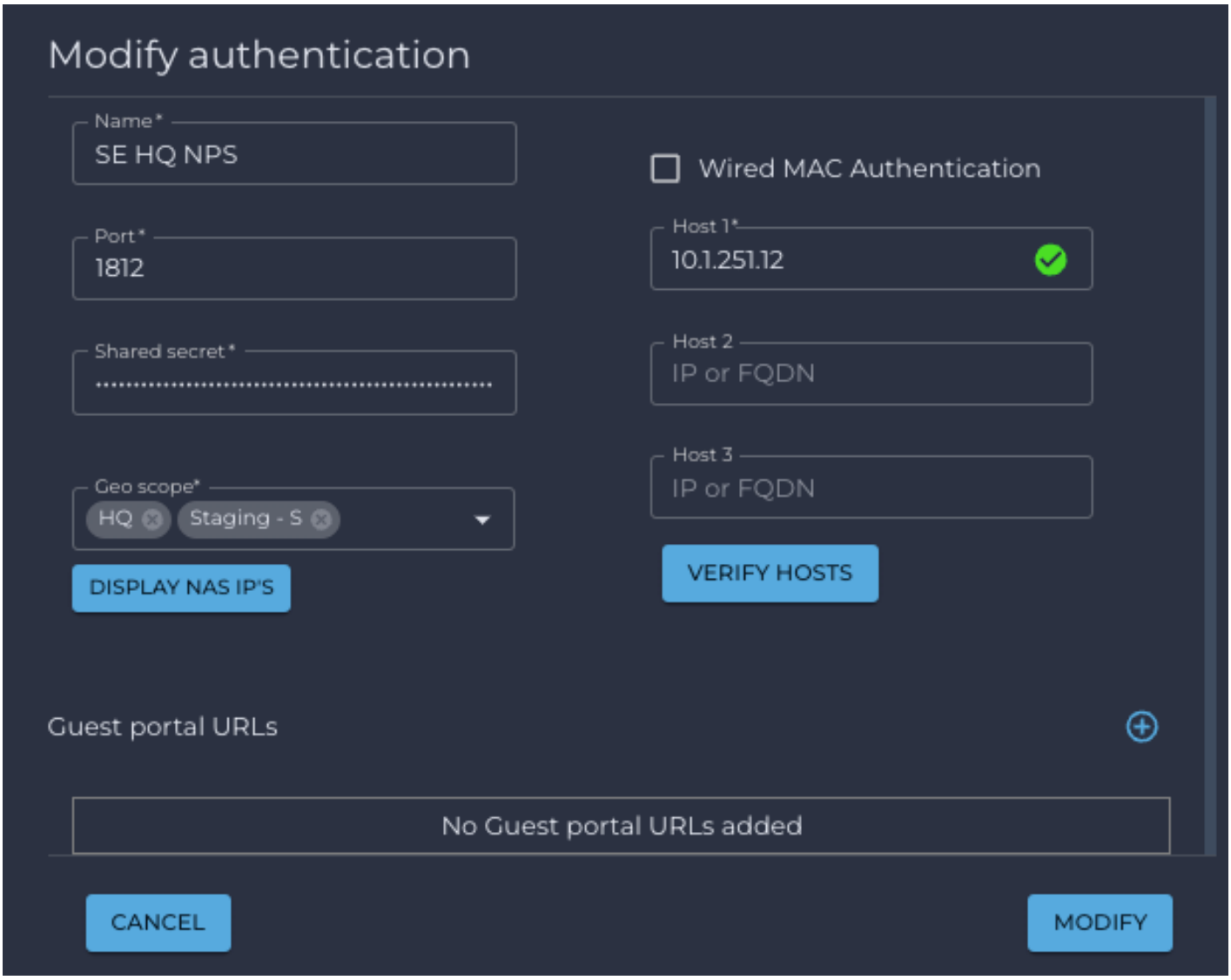
A new pop-up window opens.



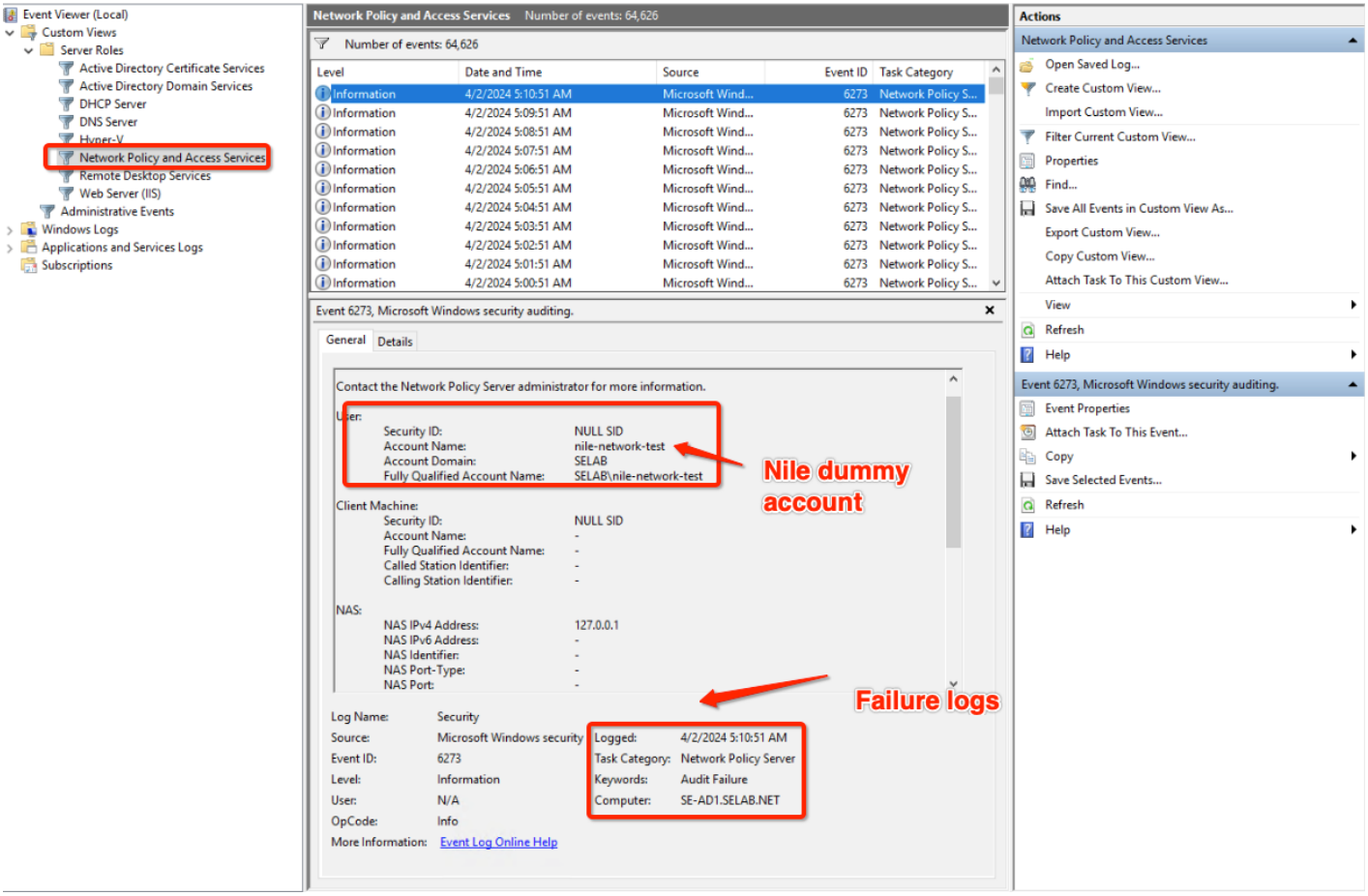
- User Id: MS Windows AD User account
- Password: User account password
- Save credentials for monitoring (Optional to use the account for Nile availability monitoring) if the testing account is not saved, Nile will use a dummy account for monitoring.
- Click on the **TEST** If the transaction fails, the IP address will be shown in red with the message “Username and password do not match”. The transaction failure will **not impact** monitoring or RADIUS functionality, this is only an indication that the RADIUS server failed to authenticate the user, to help with RADIUS authentication troubleshooting

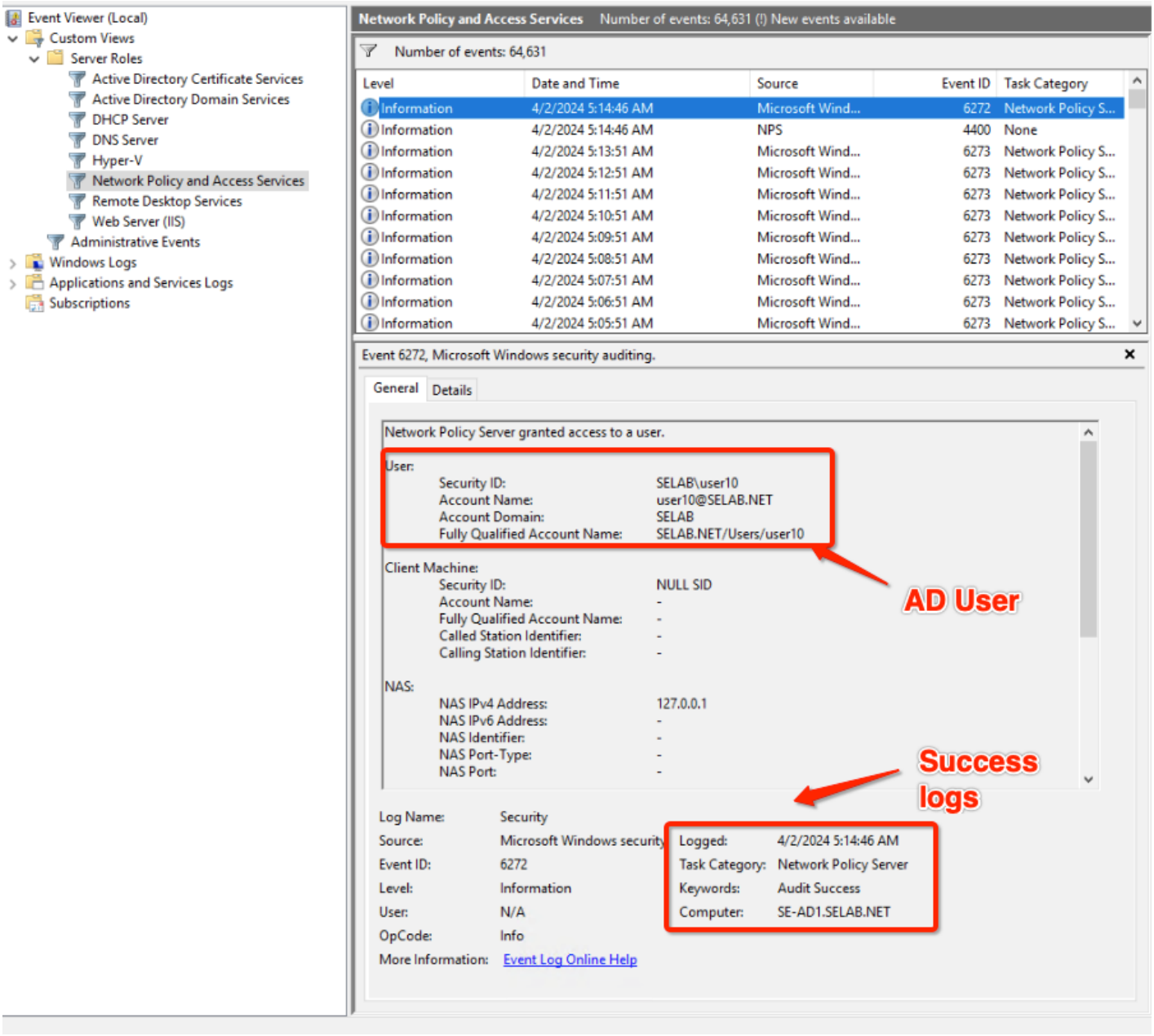


- If authentication is successful, a green circle with an arrow will display beside RADIUS host IP.



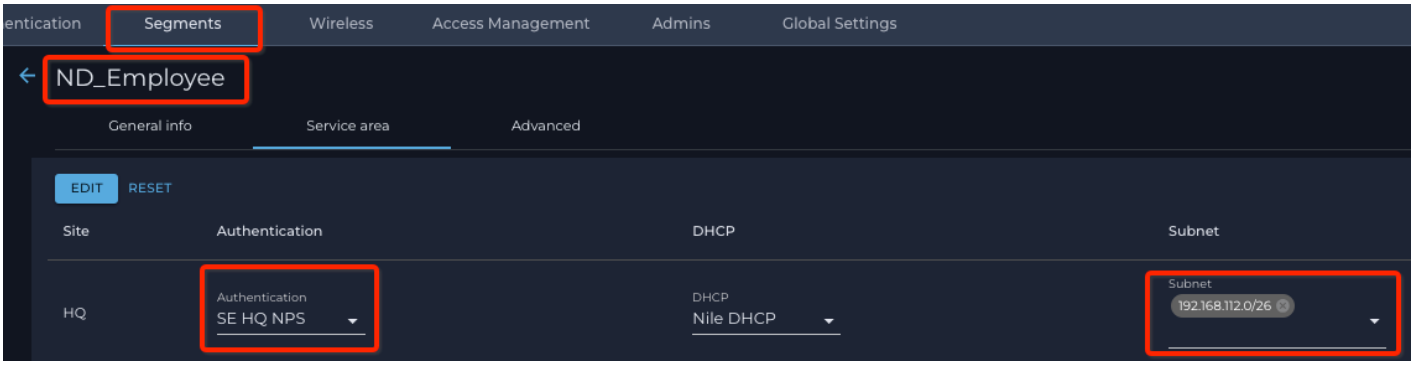
- You can verify Windows NPS logs for success or failure authentication.


Event Viewer (Local)
Custom Views
Server Roles
Active Directory Certificate Services
Active Directory Domain Services
DHCP Server
DNS Server
Hyper-V
Network Policy and Access Services
Remote Desktop Services
Web Server (IIS)
Administrative Events
Windows Logs
Applications and Services Logs
Subscriptions
Network Policy and Access Services Number of events: 64,626
Number of events: 64,626
Level Date and Time Source Event ID Task Category
Information 4/2/2024 5:10:51 AM Microsoft Wind... 6273 Network Policy S...
Information 4/2/2024 5:09:51 AM Microsoft Wind... 6273 Network Policy S...
Information 4/2/2024 5:08:51 AM Microsoft Wind... 6273 Network Policy S...
Information 4/2/2024 5:07:51 AM Microsoft Wind... 6273 Network Policy S...
Information 4/2/2024 5:06:51 AM Microsoft Wind... 6273 Network Policy S...
Information 4/2/2024 5:05:51 AM Microsoft Wind... 6273 Network Policy S...
Information 4/2/2024 5:04:51 AM Microsoft Wind... 6273 Network Policy S...
Information 4/2/2024 5:03:51 AM Microsoft Wind... 6273 Network Policy S...
Information 4/2/2024 5:02:51 AM Microsoft Wind... 6273 Network Policy S...
Information 4/2/2024 5:01:51 AM Microsoft Wind... 6273 Network Policy S...
Information 4/2/2024 5:00:51 AM Microsoft Wind... 6273 Network Policy S...
Event 6273, Microsoft Windows security auditing.
General Details
Contact the Network Policy Server administrator for more information.
User:
Security ID: NULL SID
Account Name: nile-network-test
Account Domain: SELAB
Fully Qualified Account Name: SELAB\nile-network-test
Nile dummy account
Client Machine:
Security ID: NULL SID
Account Name: -
Fully Qualified Account Name: -
Called Station Identifier: -
Calling Station Identifier: -
NAS:
NAS IPv4 Address: 127.0.0.1
NAS IPv6 Address: -
NAS Identifier: -
NAS Port-Type: -
NAS Port: -
Failure logs
Log Name: Security
Source: Microsoft Windows security
Logged: 4/2/2024 5:10:51 AM
Event ID: 6273
Task Category: Network Policy Server
Level: Information
Keywords: Audit Failure
User: N/A
Computer: SE-AD1.SELAB.NET
OpCode: Info
More Information: Event Log Online Help
Actions
Network Policy and Access Services
Open Saved Log...
Create Custom View...
Import Custom View...
Filter Current Custom View...
Properties
Find...
Save All Events in Custom View As...
Export Custom View...
Copy Custom View...
Attach Task To This Custom View...
View
Refresh
Help
Event 6273, Microsoft Windows security auditing.
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help

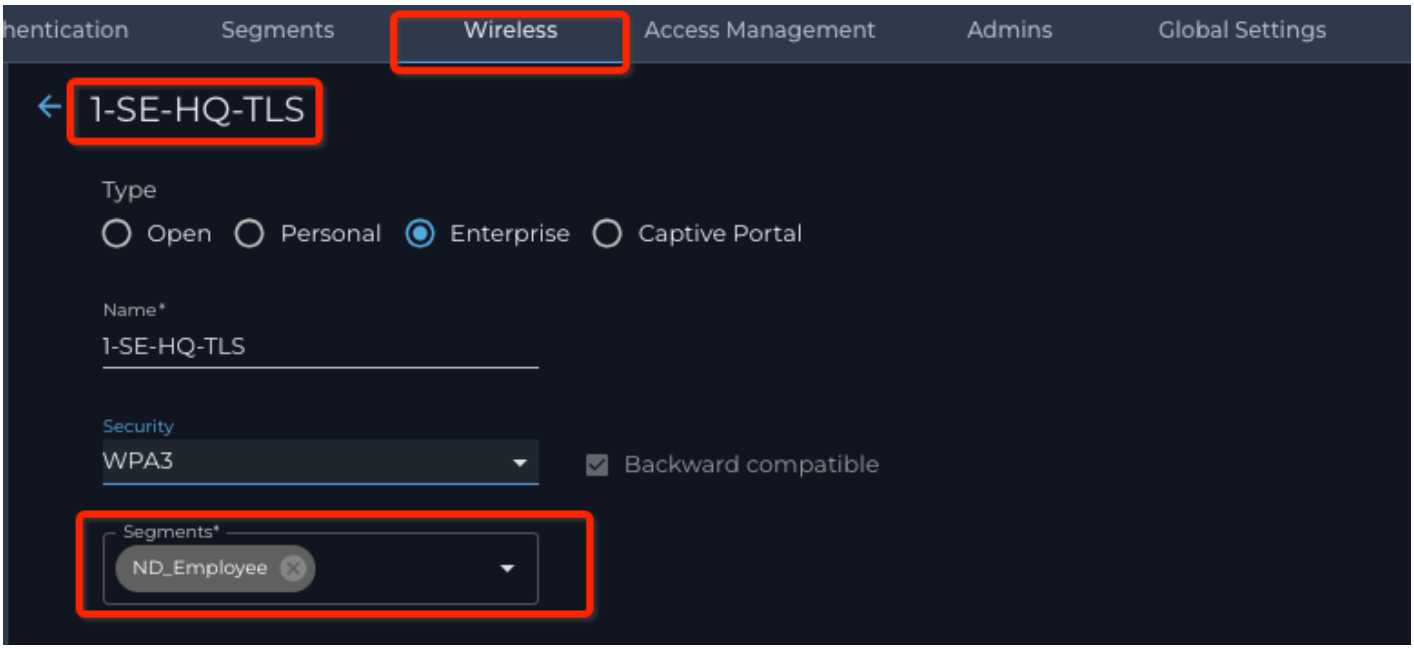


Configuring Nile Segments and Wireless SSIDs (RADIUS)

- Log onto Nile Portal: https://u1.nile-global.cloud/
- Navigate to **Nile Portal ? Setting** button ? **Segments** tab
- Click on ? button; this opens a new Segment configuration panel
- In the **General info** sub-tab, enter a name in the “Name” field.
- Navigate to **Nile Portal ? Setting** button ? **Segments** tab ? **Service area** sub-tab
- Click the **SELECT SERVICE AREAS** button
- Select (1) all sites, (2) one site, or (3) one zone, using the radio buttons and associated lists
- Select the authentication server from the Authentication pull-down list.
- Select the DHCP server from the DHCP pull-down list.
- Select the subnet(s) from the Subnet pull-down list — you may select one or more
- Click the **SAVE** button.



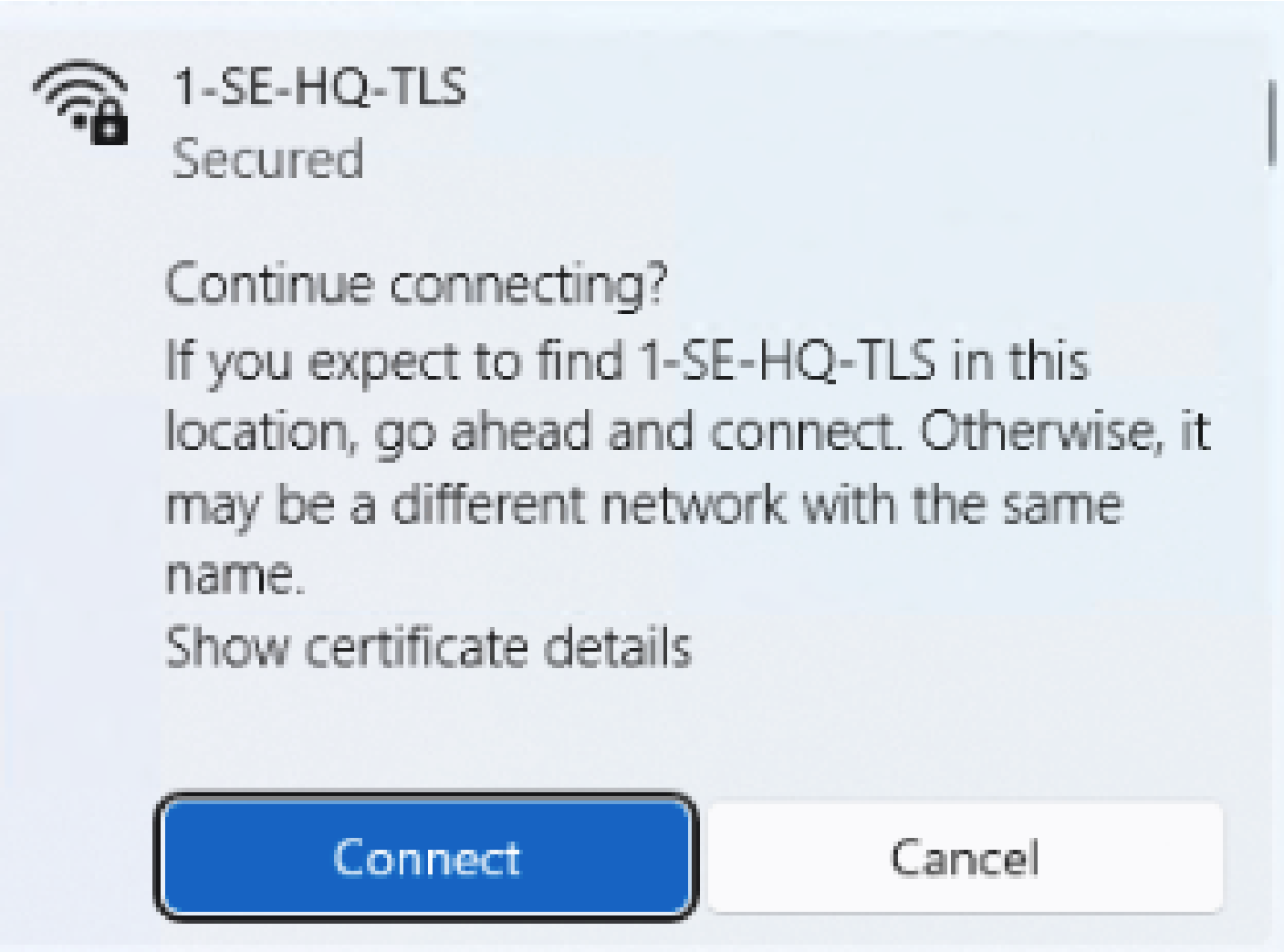
- Navigate to **Nile Portal ? Setting** button ? **Wireless** tab
- Click on ? button; this creates a new SSID
- Click the Enterprise radio button
- Enter the Name for the SSID: this will be what the APs will use as a beacon
- Select the security type from the Security pull-down list
- Select the segment created earlier. (Example ND_Employee segment)
- Verify that you have entered the correct information



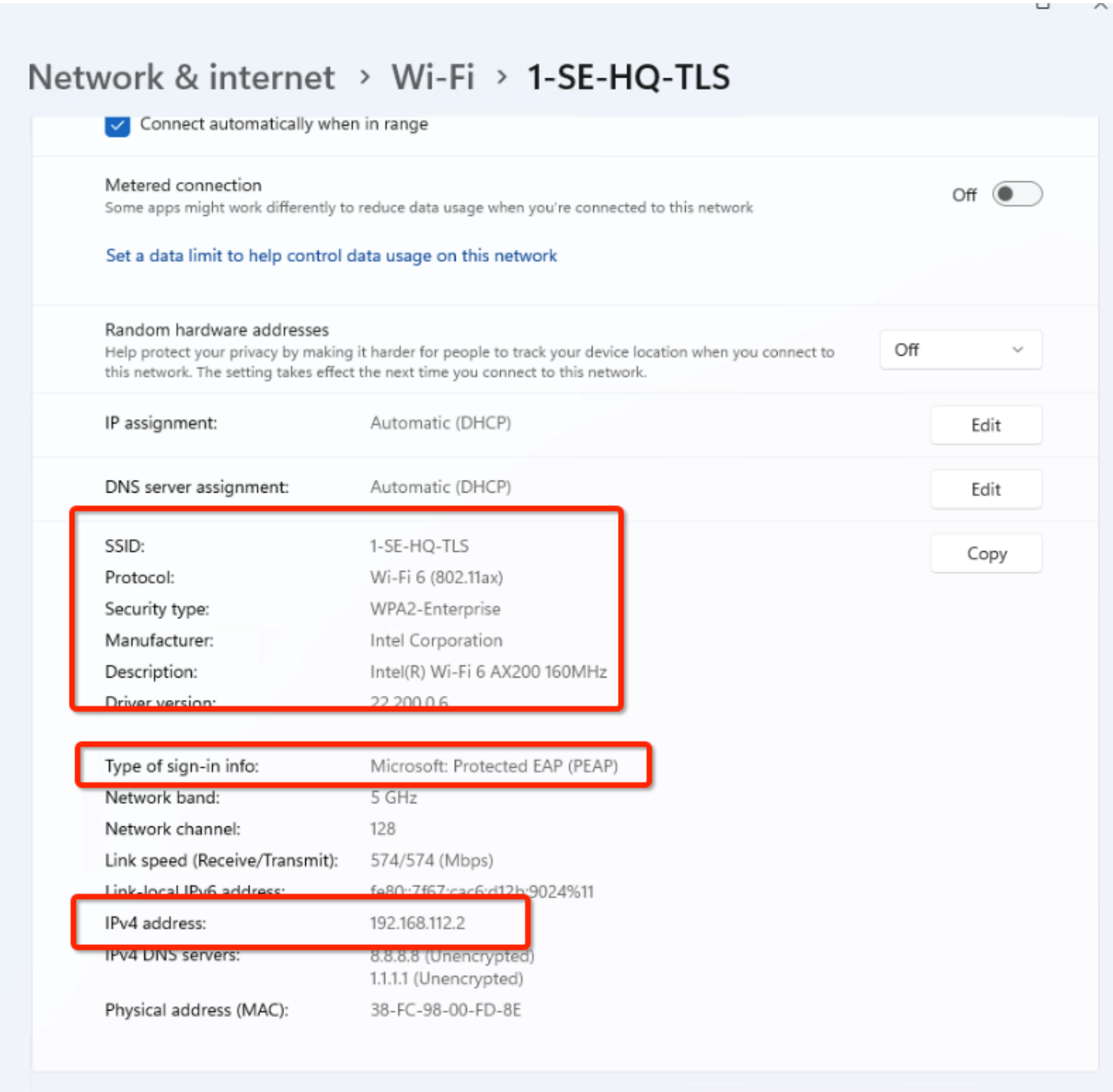
- Press the **SAVE** button

Microsoft NPS Wireless 802.1x Connection Test

- From a Wireless-capable client device, select Nile 802.1x SSID; log in using a domain user member; and, verify that device connects to the SSID.Note: First-time clients need to accept the certificate and connect to the network using 802.1x; user needs to click on the **Connect** button to continue.

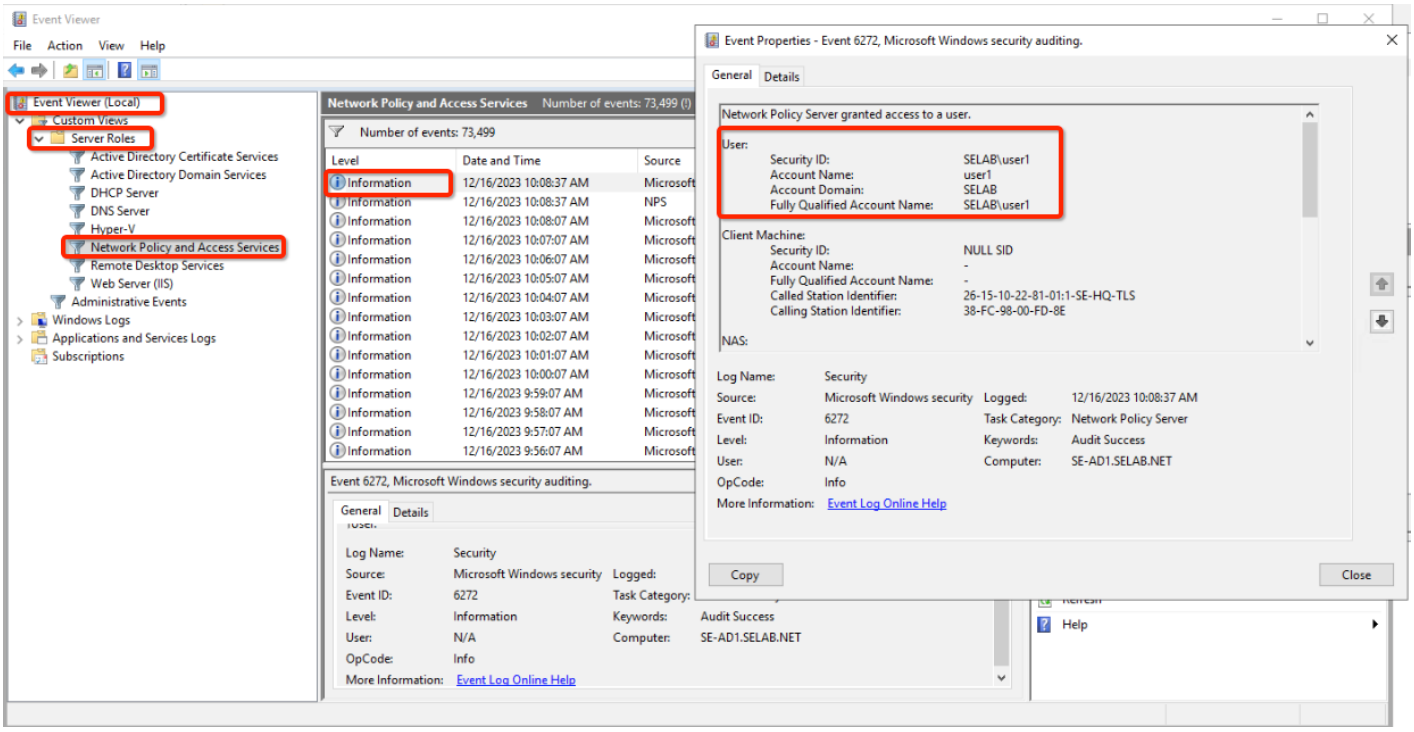


- Verify sign-in info and IP address. IP needs to be from segment subnet range; in our example 192.168.112.0/26 for ND_Employee



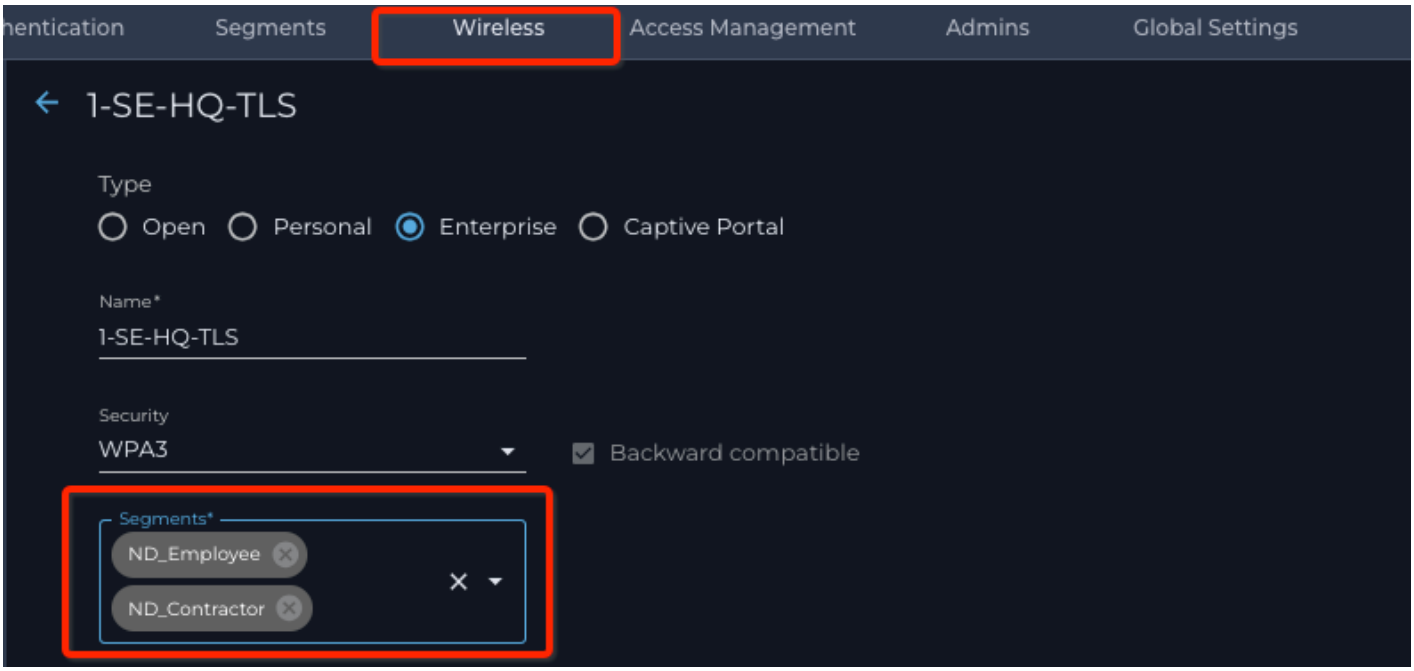
Verify NPS logs:

- Open Event Viewer, and then, under Custom views, select **Server Roles ® Network Policy and Access Services**
- If needed, filter for events that have Event ID 6273 or 6274. Most authentication failures produce these events.

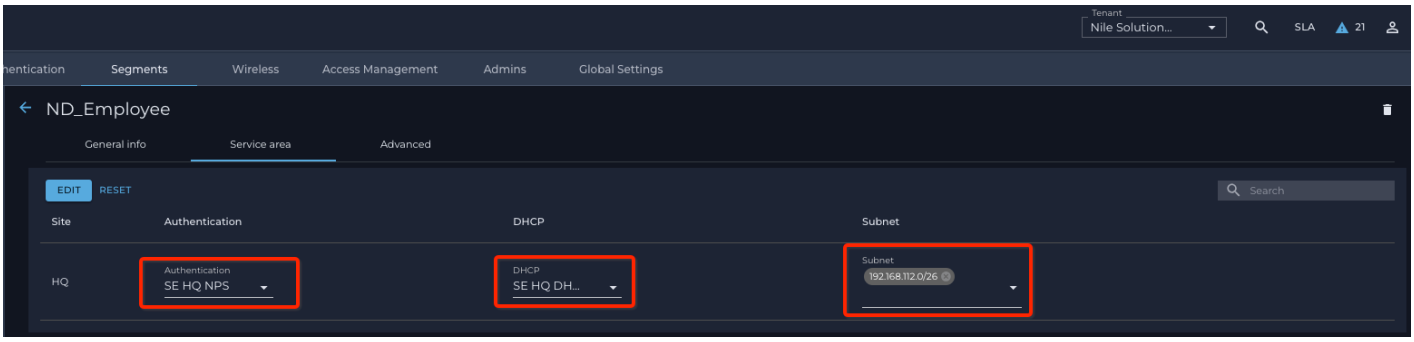


Nile Segment mapping with Microsoft NPS Radius Server

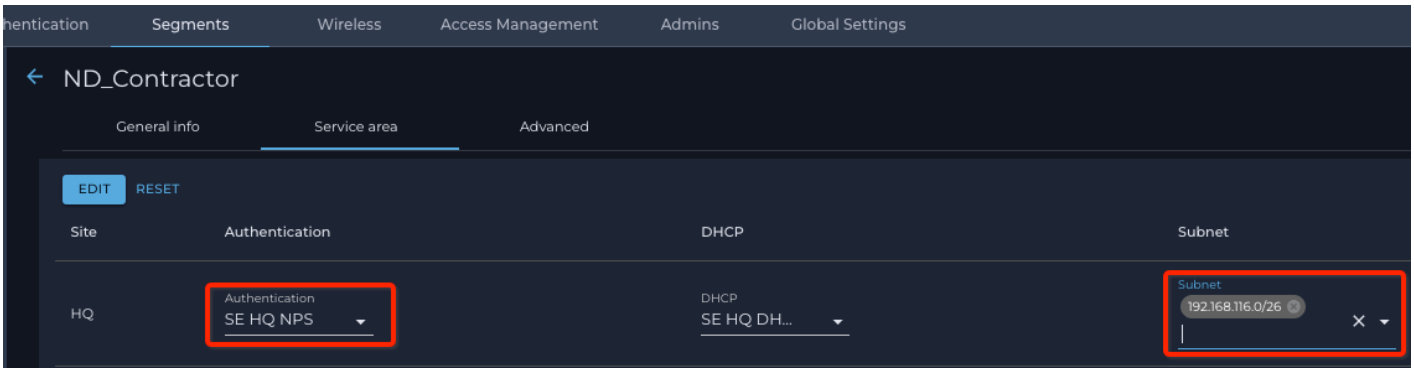
- Log onto Nile Portal: https://u1.nile-global.cloud/
- Navigate to **Nile Portal ? Settings** button ? **Wireless** tab
- Click on the ? (edit) icon next to the name of the SSID, to edit the wireless SSID
- Add an additional segment from the drop-down list.



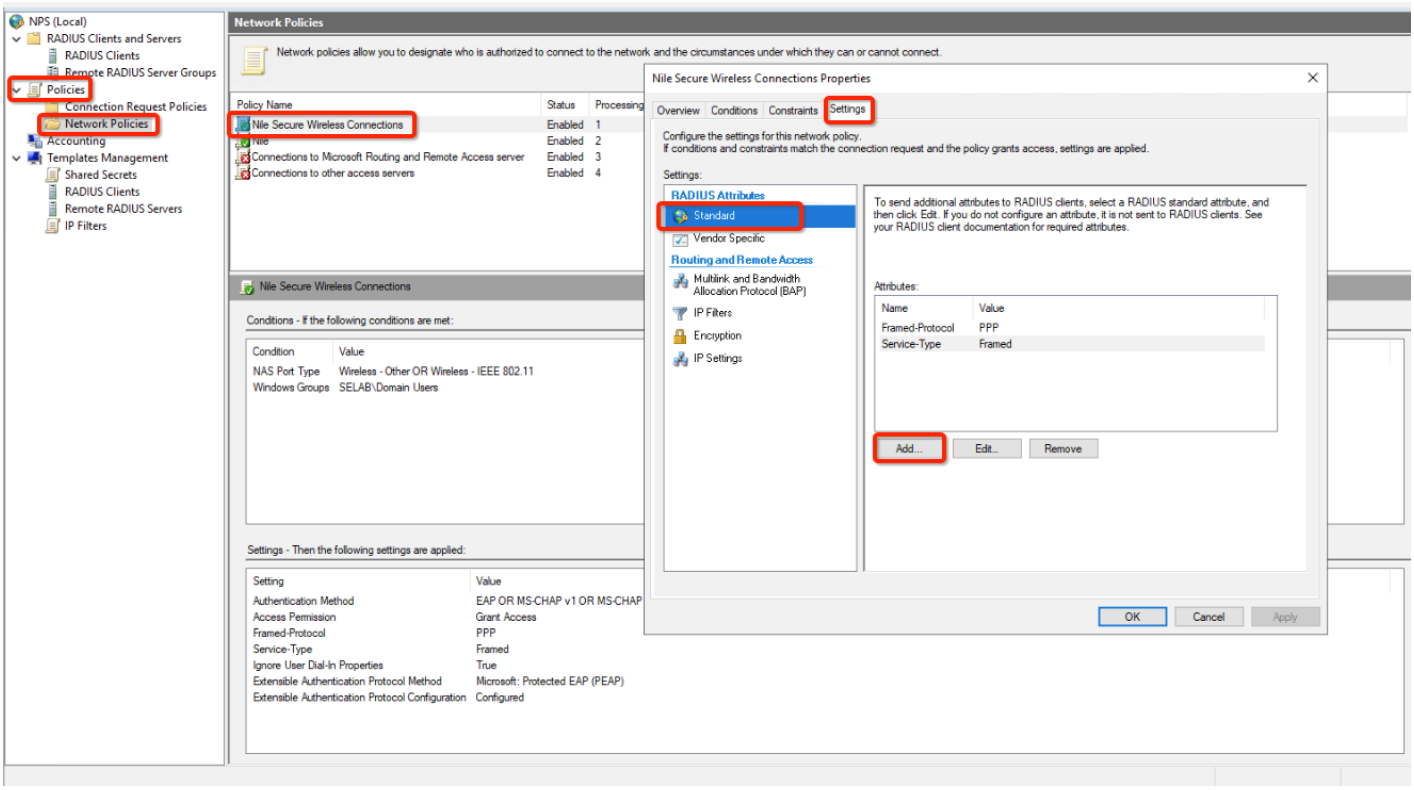
You may need to go back at look at the definitions of the segments in your list. In this example (Nile Portal ® **Settings** button ? **Segments** tab ? edit ssid **“**ND_Employee” ® **Service area** subtab),
“segment ND_Employee” is configured with Microsoft NPS as an authentication server and IP address Subnet 192.168.112.0/26:



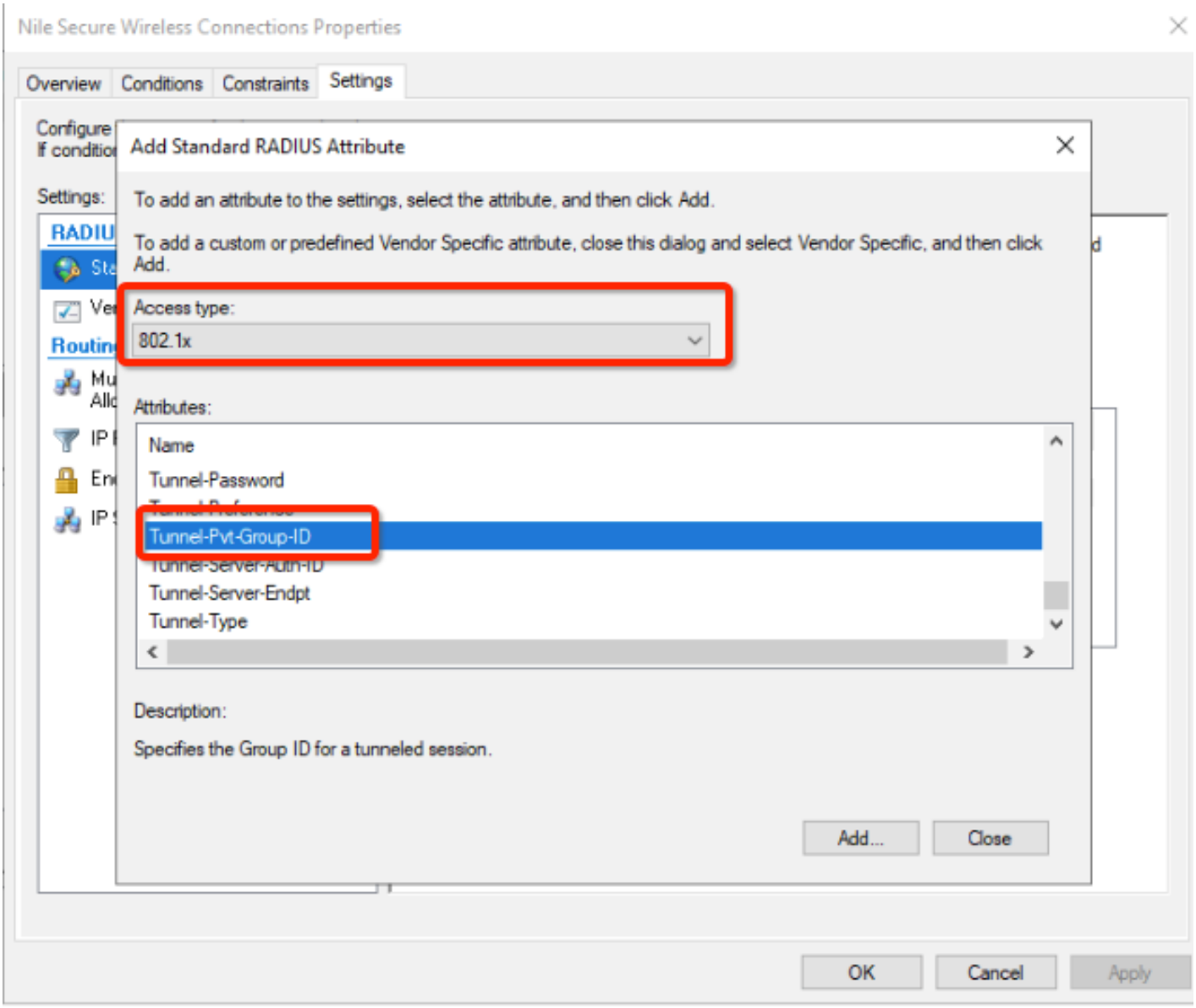
and
(Nile Portal ® **Settings** button ® **Segments** tab ® edit ssid **“**ND_Contractor” ® **Service area** subtab)
segment “ND_Contractor” is configured with Microsoft NPS as an authentication server and IP address Subnet 192.168.116.0/26:



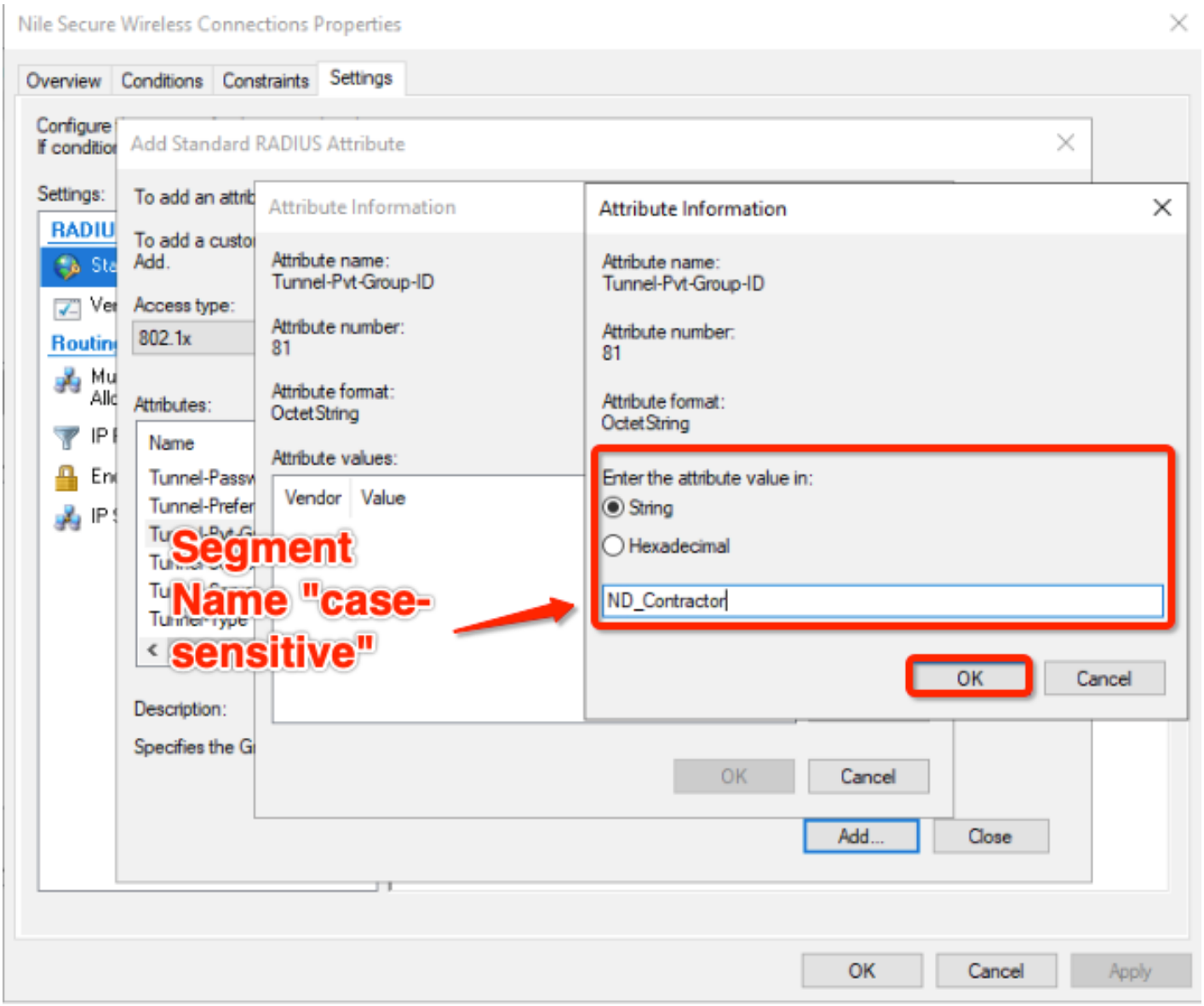
- In the Console, navigate to NPS (Local) ® Policies ® Select your Policy”
- Click on the Edit button.
- Select Setting ® Standard
- click on the **Add** button.



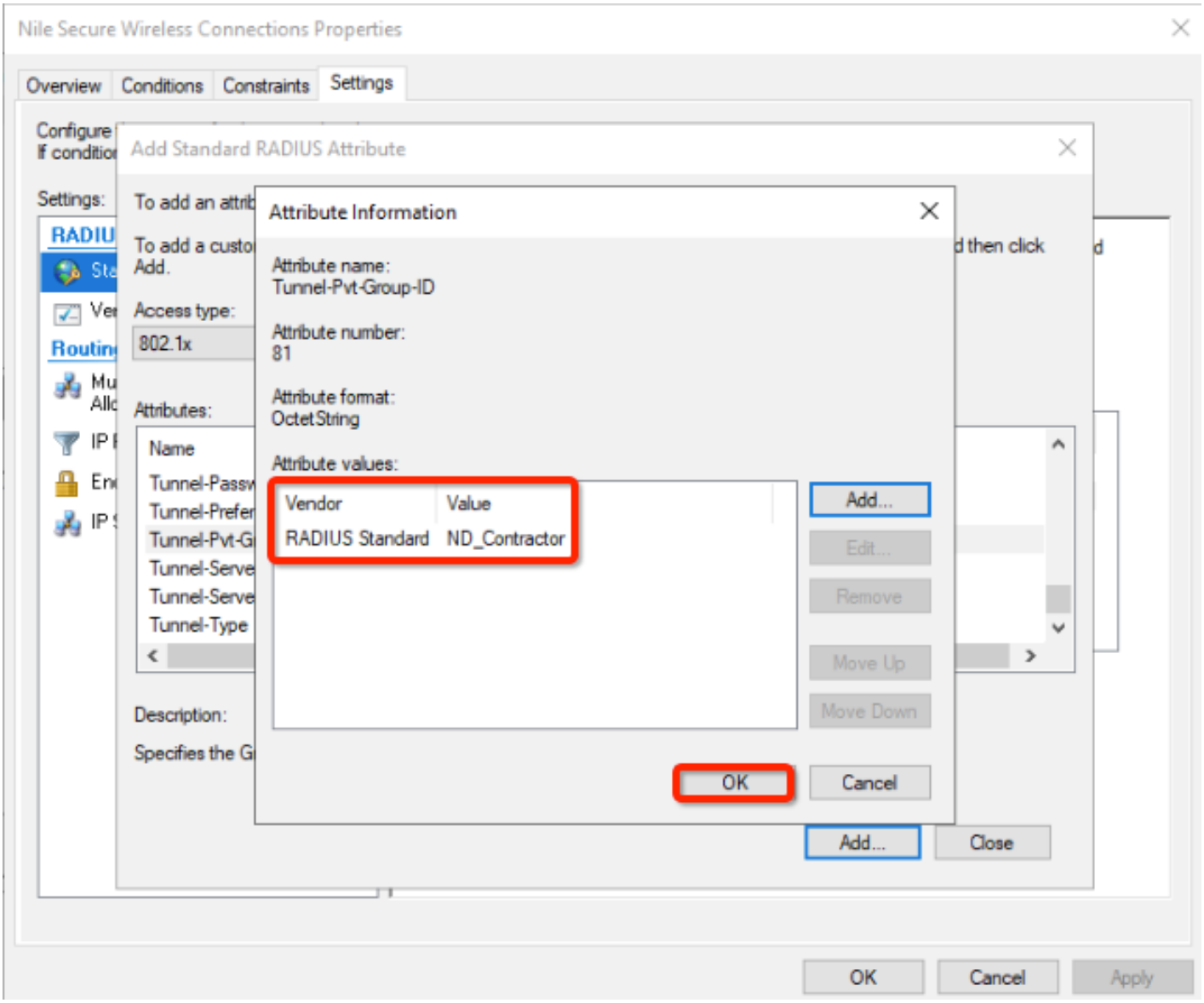
- From the **Access Type** drop-down list, select “802.1x”
- Click on attribute **Tunnel-Pvt-Group-ID** in the Attributes window
- This will use the tunnel group ID RADIUS standard attribute to assign Nile segment name to policy members.



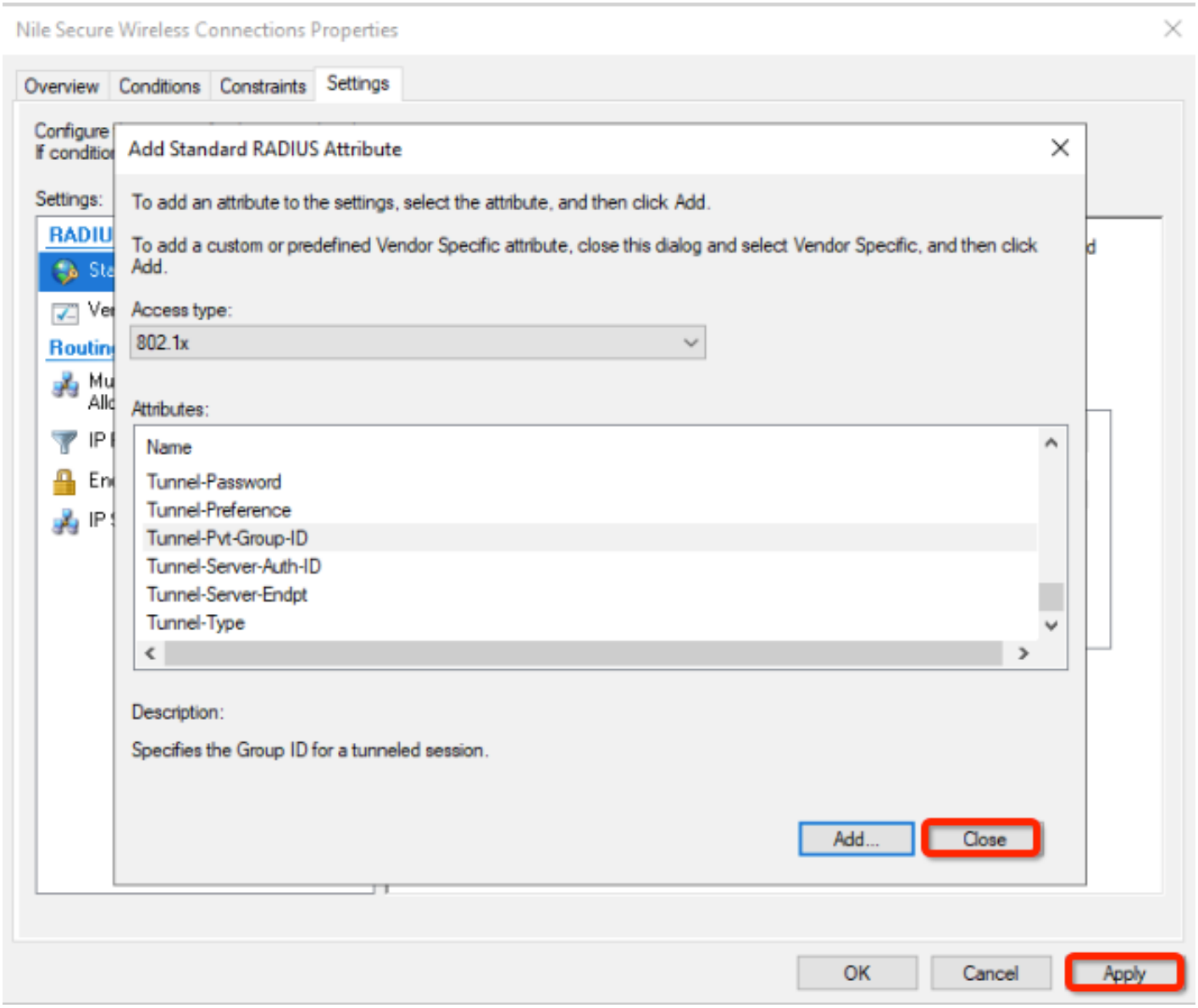
- In Attribute Information, click the **String** radio button
- Enter the segment name into the value field for the attribute. The segment name is case sensitive.



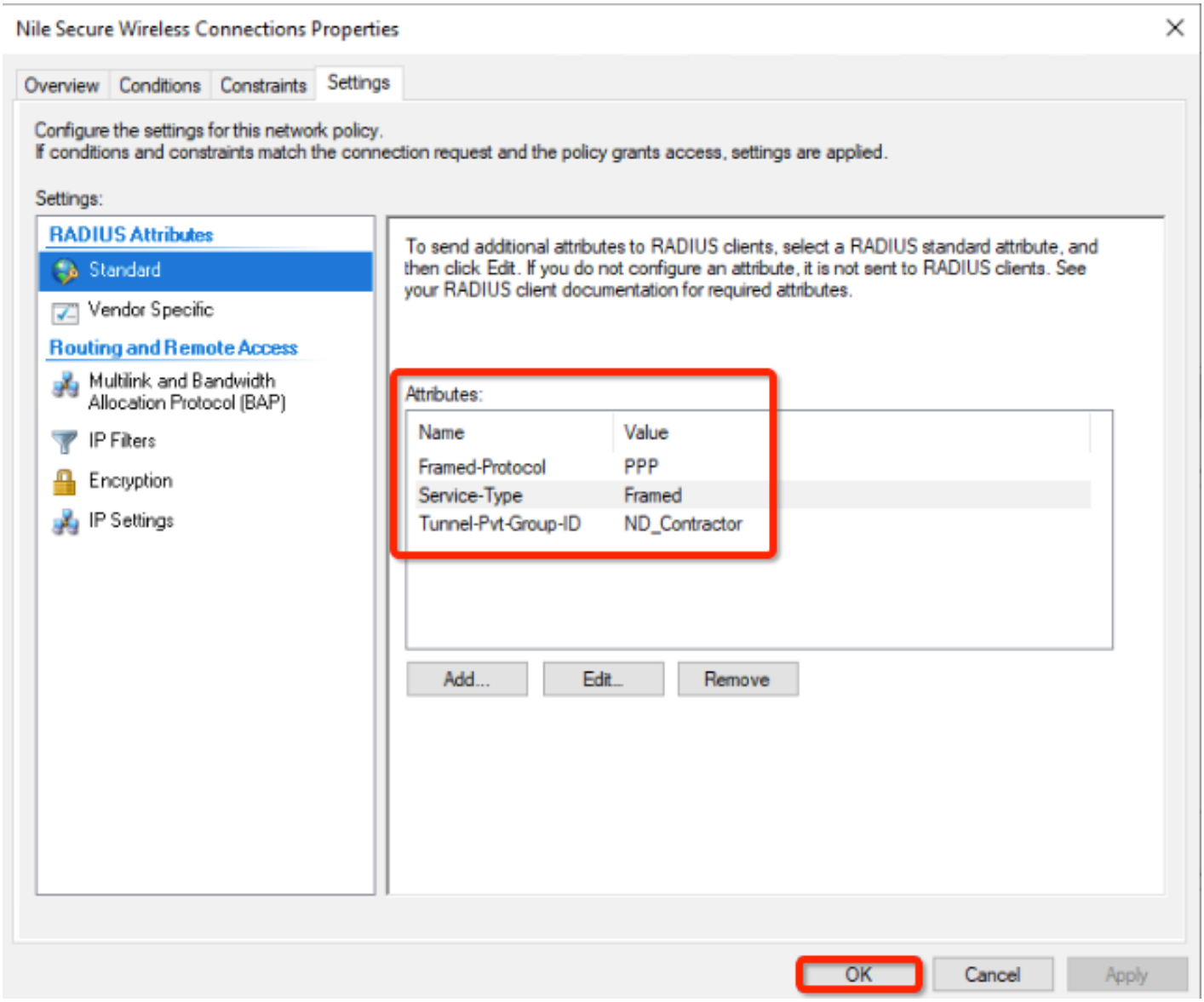
- Click on the **OK** button, to add Tunnel0Pvt-Group-ID attribute



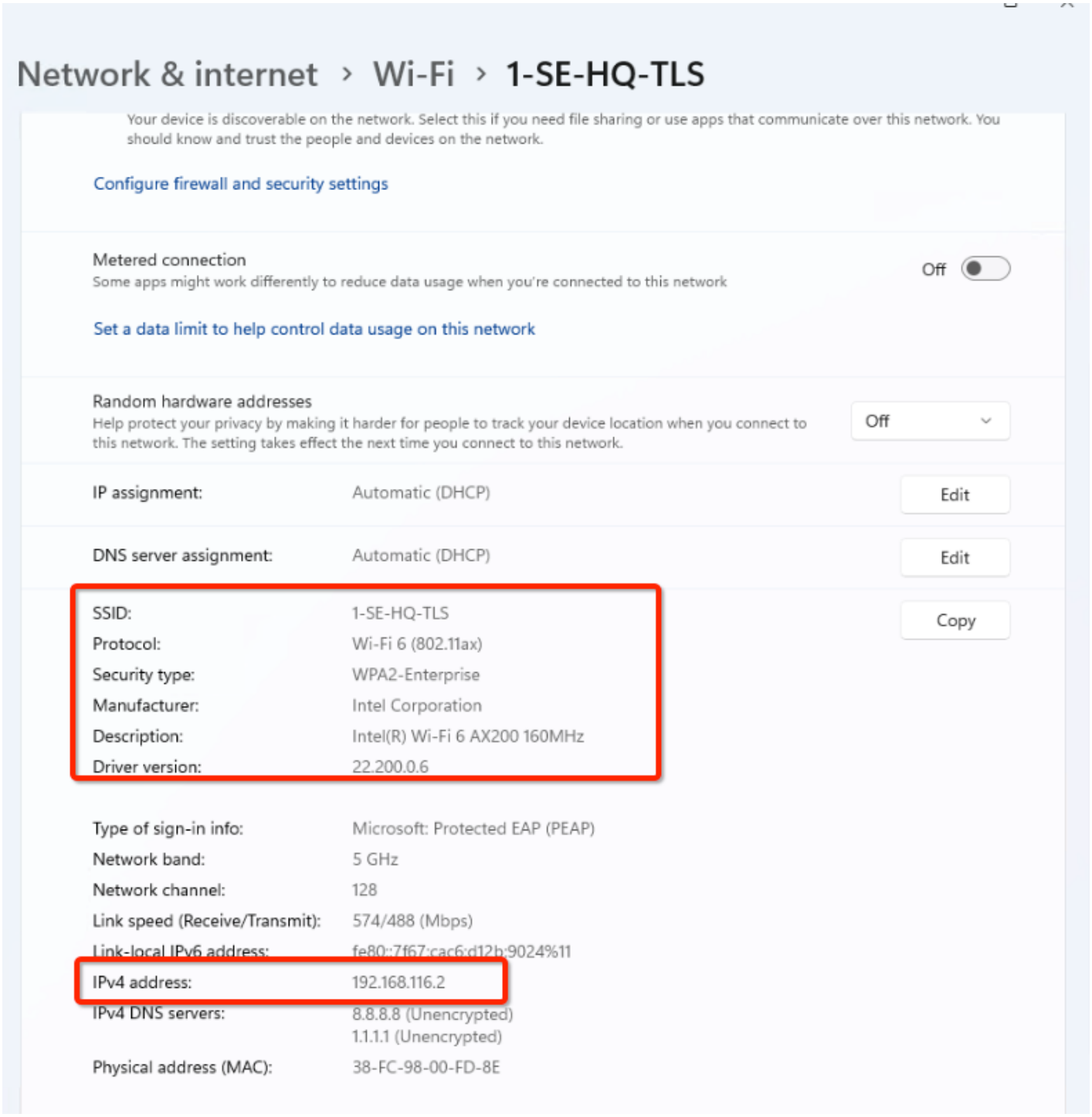
- Click the **Close** button



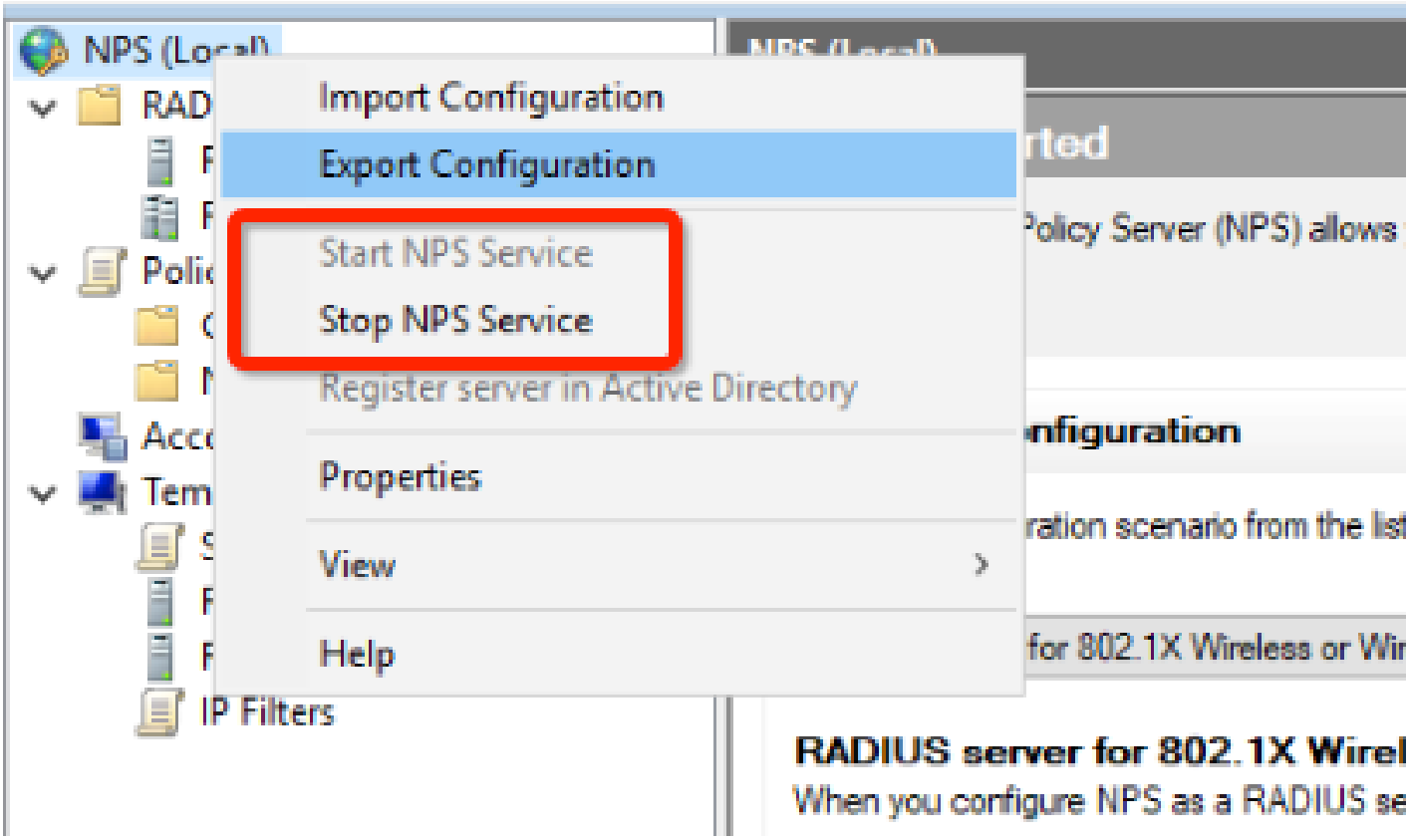
- Verify RADIUS standard attributes.
- Click the **OK** button



- Verify sign-in info and IP address. IP needs to be from segment subnet rang (in our example 192.168.116.0/26 for ND_Contractor)



Note: NPS is a Microsoft Windows service. Adding or changing configs might require restarting the service. To restart, in the Console, navigate to NPS (Local), right-click on NPS (local), select Stops NPS Service to stop NPS and then select Start NPS Service.


NPS (Local)
RAD
Polic
Acc
Tem
IP Filters
Import Configuration
Export Configuration
Start NPS Service
Stop NPS Service
Register server in Active Directory
Properties
View
Help
rted
olicy Server (NPS) allows
nfiguration
ration scenario from the list
for 802.1X Wireless or Wir
RADIUS server for 802.1X Wirel
When you configure NPS as a RADIUS se