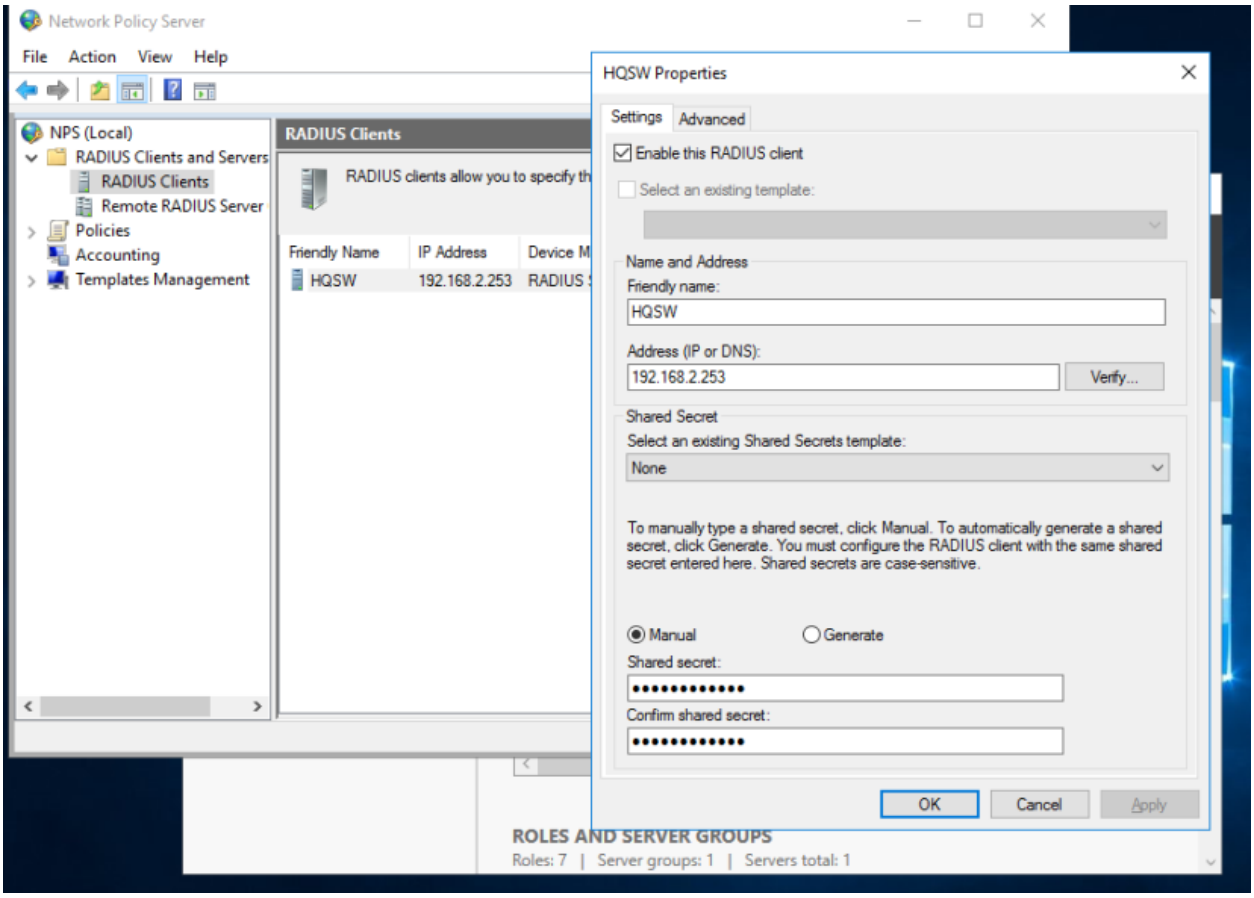
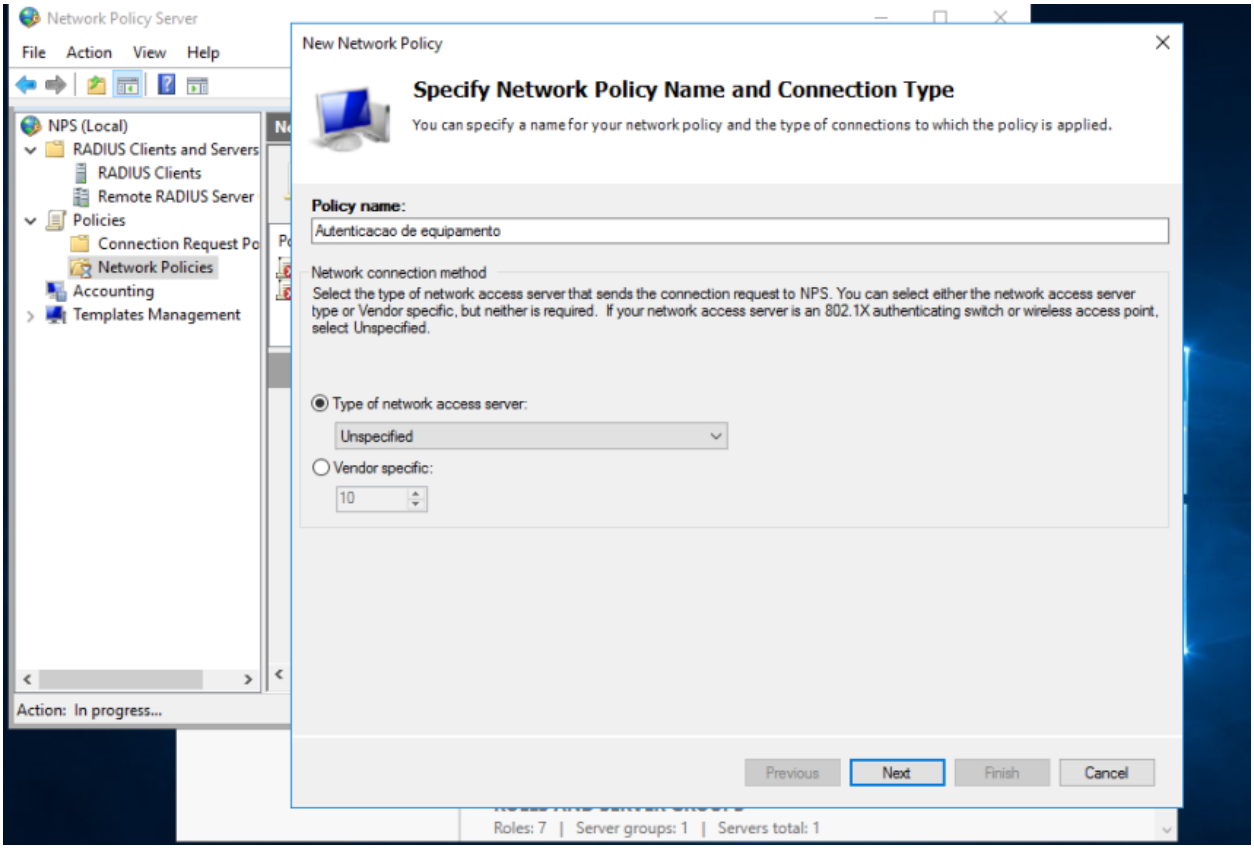
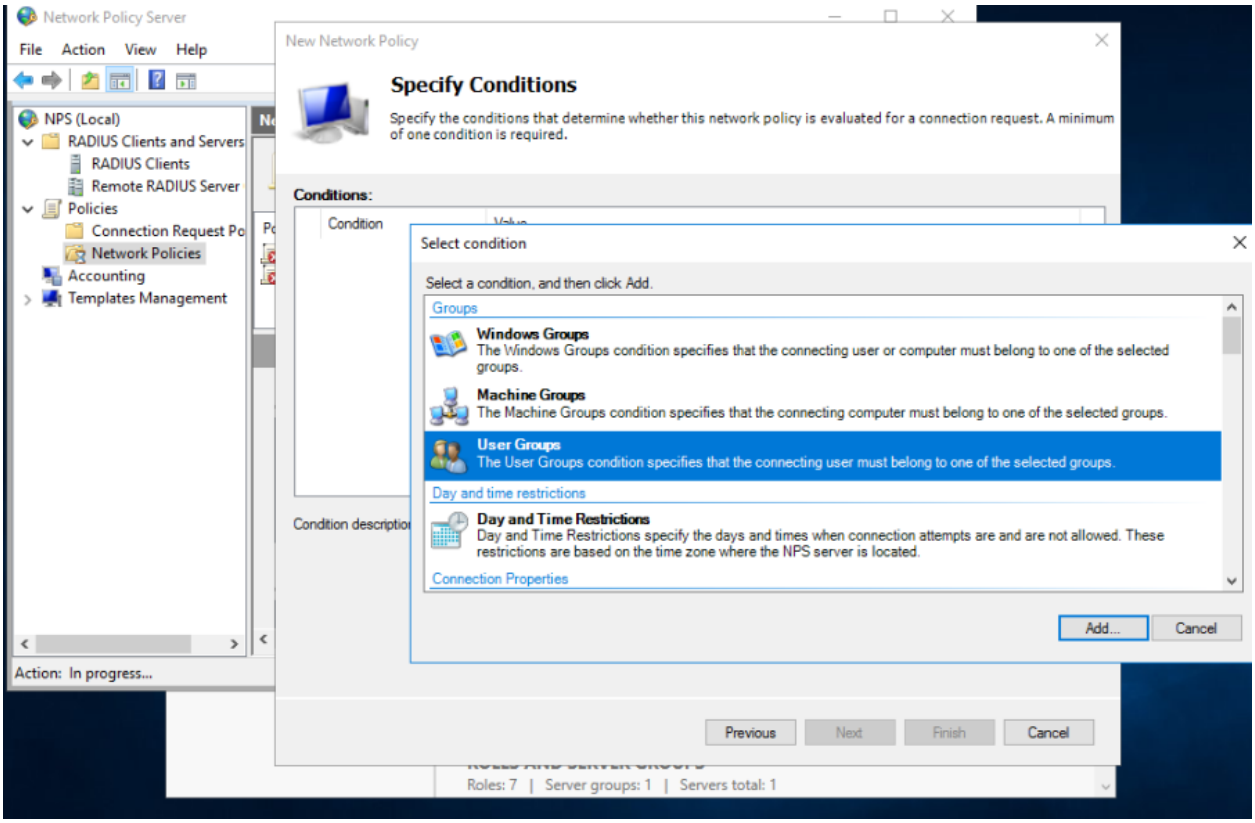
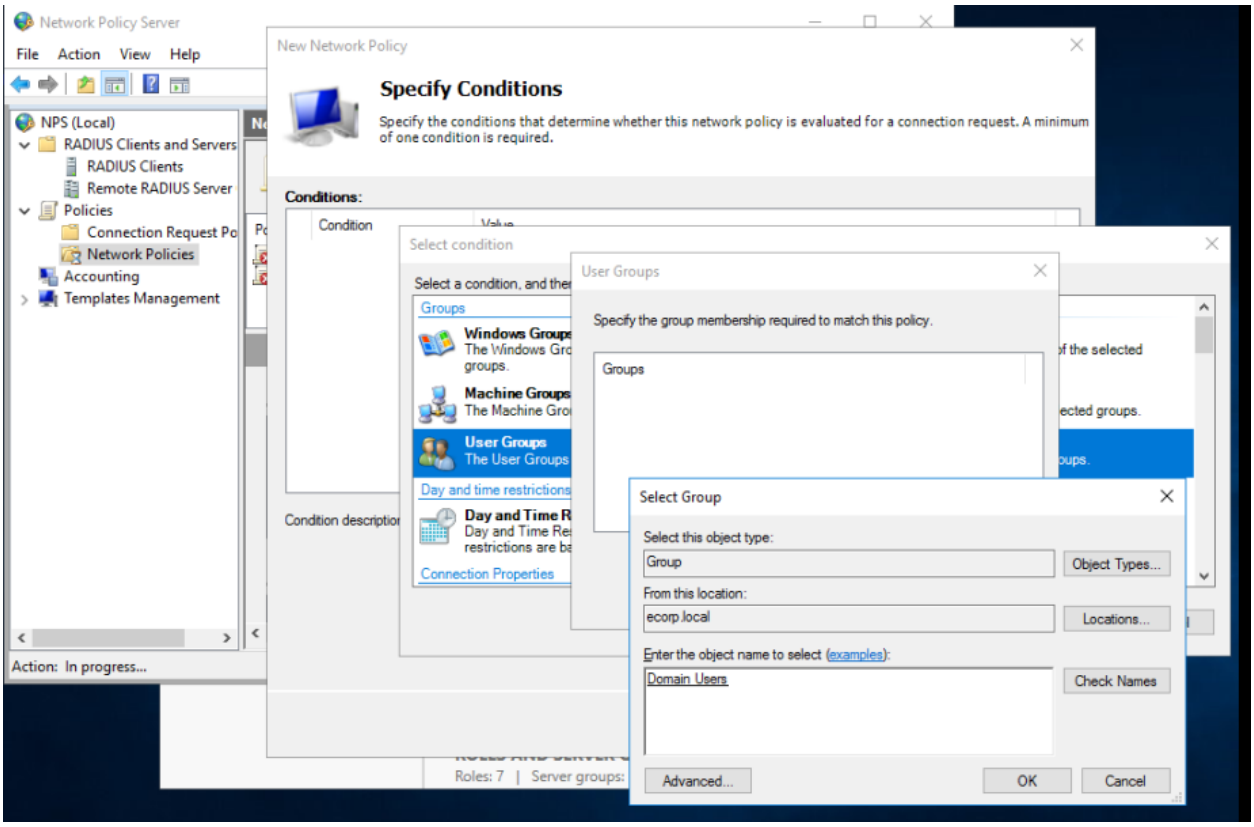
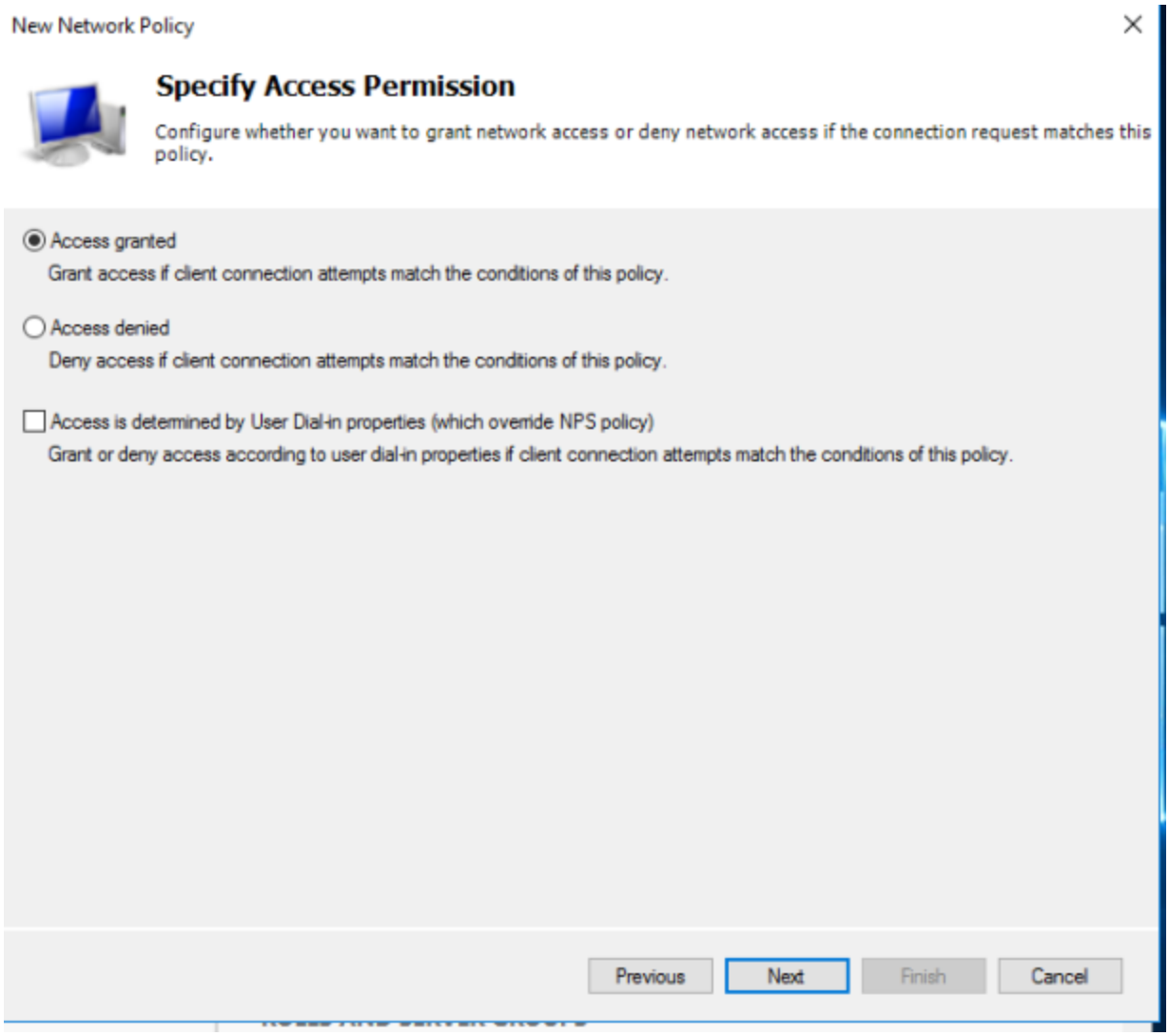
# RADIUS (NPS)

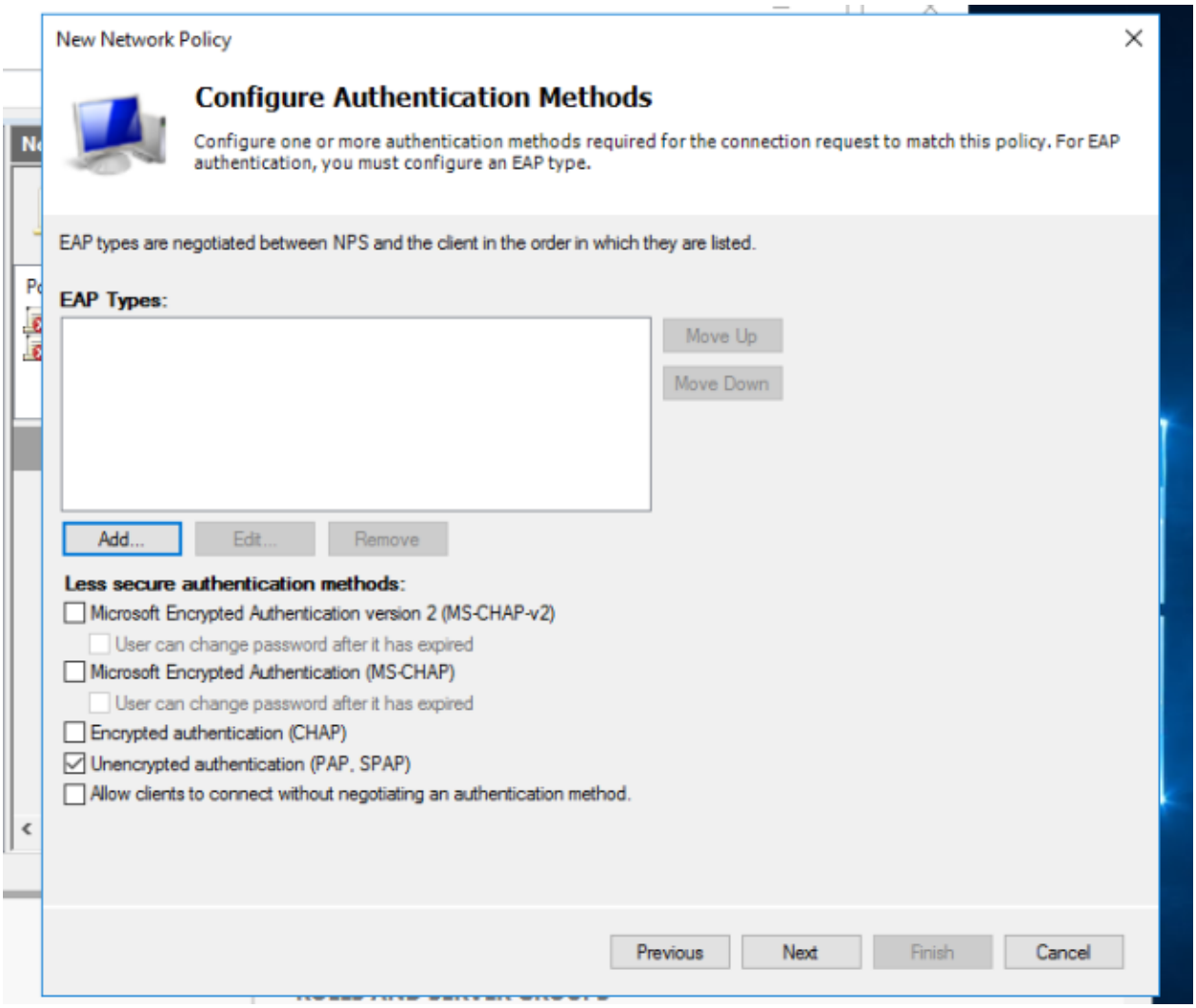

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server
Policies
Accounting
Templates Management
RADIUS Clients
RADIUS clients allow you to specify th
Friendly Name
IP Address
Device M
HQSW
192.168.2.253
RADIUS
HQSW Properties
Settings
Advanced
Enable this RADIUS client
Select an existing template:
Name and Address
Friendly name:
HQSW
Address (IP or DNS):
192.168.2.253
Verify...
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
ROLES AND SERVER GROUPS
Roles: 7 | Server groups: 1 | Servers total: 1

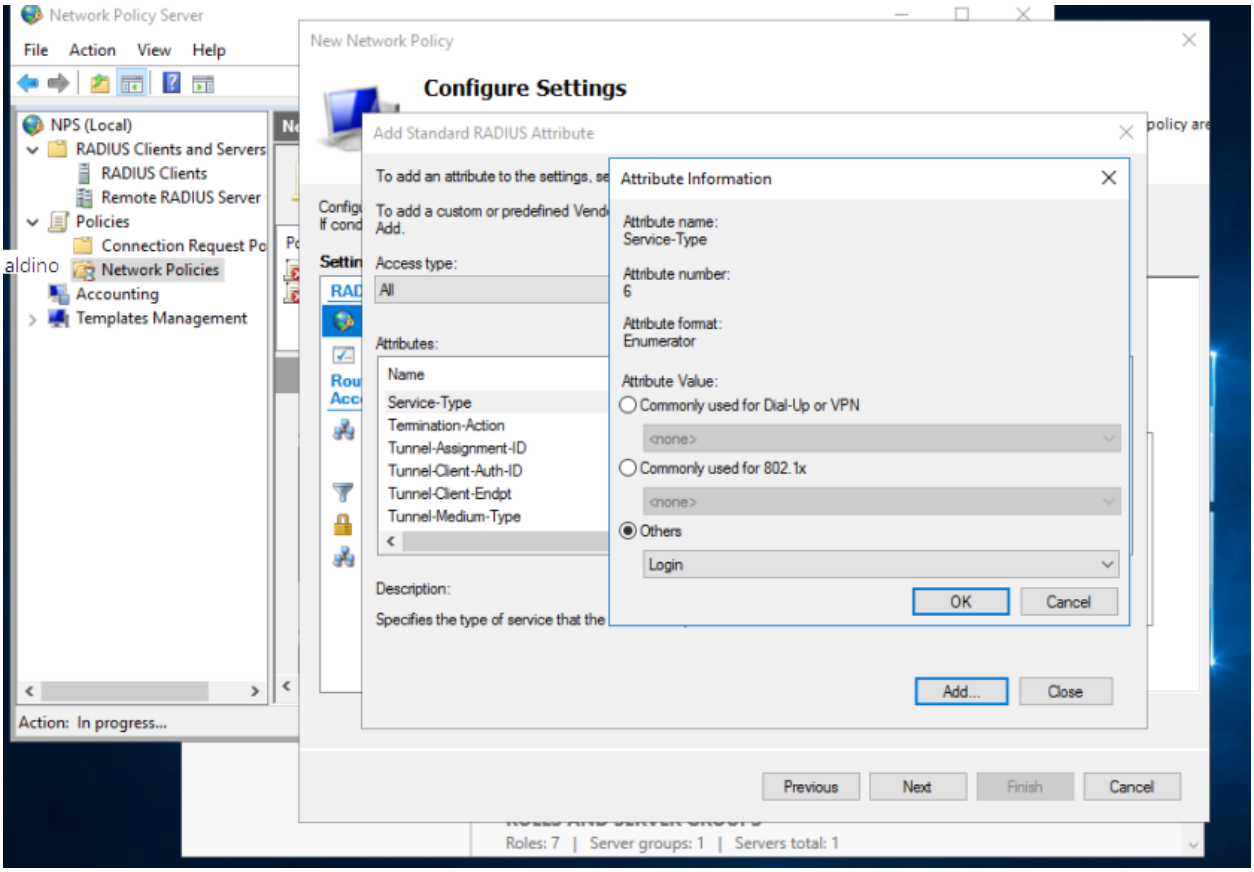

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server
Policies
Connection Request Po
Network Policies
Accounting
Templates Management
Action: In progress...
New Network Policy
Specify Network Policy Name and Connection Type
You can specify a name for your network policy and the type of connections to which the policy is applied.
Policy name:
Autenticacao de equipamento
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
Roles: 7 | Server groups: 1 | Servers total: 1


Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server
Policies
Connection Request Po
Network Policies
Accounting
Templates Management
Action: In progress...
New Network Policy
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
Condition descriptio
Select condition
Select a condition, and then click Add.
Groups
Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.
Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.
User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.
Day and time restrictions
Day and Time Restrictions
Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.
Connection Properties
Add...
Cancel
Previous
Next
Finish
Cancel
Roles: 7 | Server groups: 1 | Servers total: 1

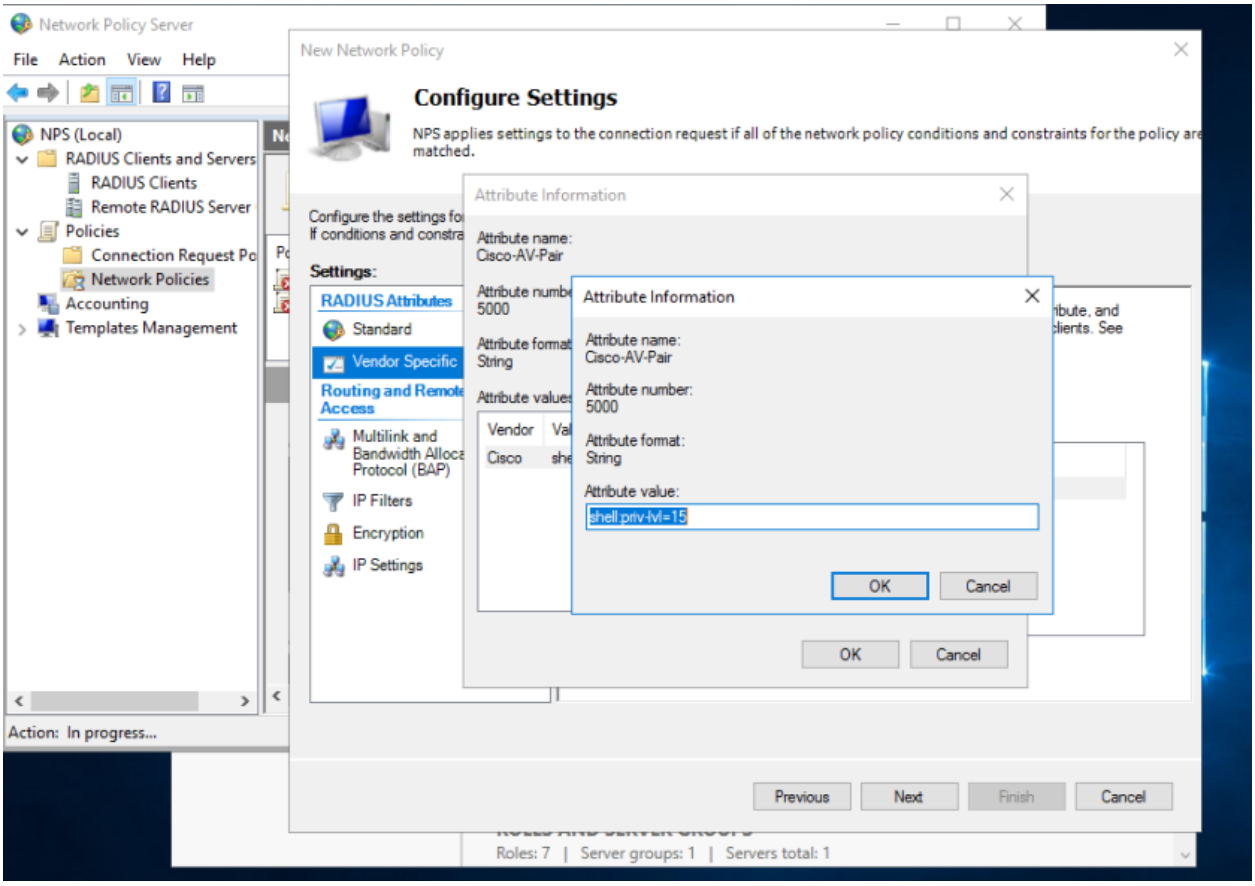

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server
Policies
Connection Request Po
Network Policies
Accounting
Templates Management
Action: In progress...
New Network Policy
Specify Conditions
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.
Conditions:
Condition
Select condition
Select a condition, and ther
Groups
Windows Groups
The Windows Gro
groups.
Machine Groups
The Machine Gro
User Groups
The User Groups
Day and time restrictions
Day and Time R
Day and Time Re
restrictions are ba
Connection Properties
User Groups
Specify the group membership required to match this policy.
Groups
Select Group
Select this object type:
Group
Object Types...
From this location:
ecorp.local
Locations...
Enter the object name to select (examples):
Domain Users
Check Names
Advanced...
OK
Cancel
Roles: 7 | Server groups:

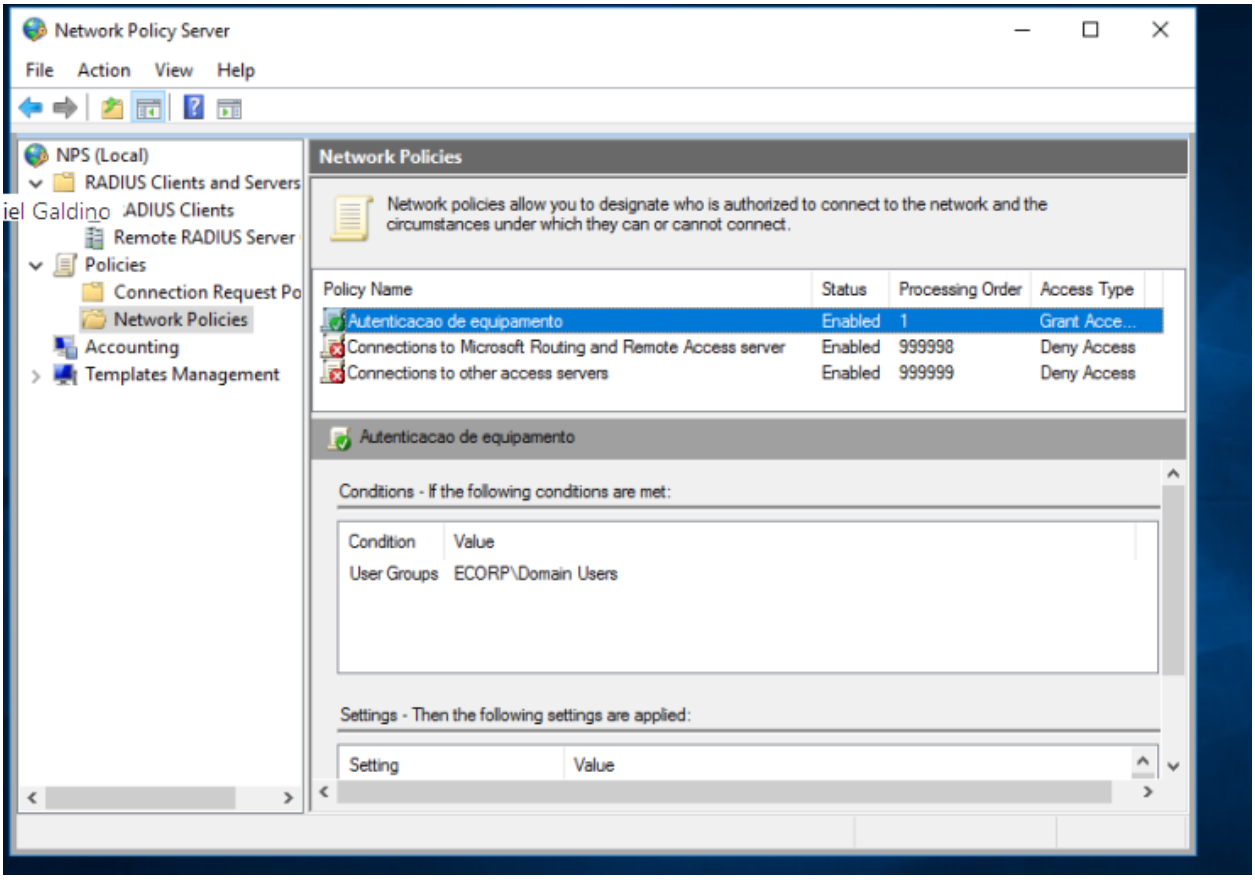

New Network Policy
Specify Access Permission
Configure whether you want to grant network access or deny network access if the connection request matches this policy.
Access granted
Grant access if client connection attempts match the conditions of this policy.
Access denied
Deny access if client connection 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.
Previous
Next
Finish
Cancel


New Network Policy
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.
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.
Previous
Next
Finish
Cancel




shell:priv-lvl=15


Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server
Policies
Connection Request Po
Network Policies
Accounting
Templates Management
Action: In progress...
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 fo
If conditions and constra
Settings:
RADIUS Attributes
Standard
Vendor Specific
Routing and Remote Access
Multilink and Bandwidth Alloca Protocol (BAP)
IP Filters
Encryption
IP Settings
Attribute Information
Attribute name:
Cisco-AV-Pair
Attribute numbe
5000
Attribute format
String
Attribute values
Vendor
Cisco
Attribute Information
Attribute name:
Cisco-AV-Pair
Attribute number:
5000
Attribute format:
String
Attribute value:
shell:priv-lvl=15
OK
Cancel
OK
Cancel
Previous
Next
Finish
Cancel
Roles: 7 | Server groups: 1 | Servers total: 1


Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
ADIUS Clients
Remote RADIUS Server
Policies
Connection Request Po
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
Autenticacao de equipamento
Enabled
1
Grant Acce...
Connections to Microsoft Routing and Remote Access server
Enabled
999998
Deny Access
Connections to other access servers
Enabled
999999
Deny Access
Autenticacao de equipamento
Conditions - If the following conditions are met:
Condition
Value
User Groups
ECORP\Domain Users
Settings - Then the following settings are applied:
Setting
Value