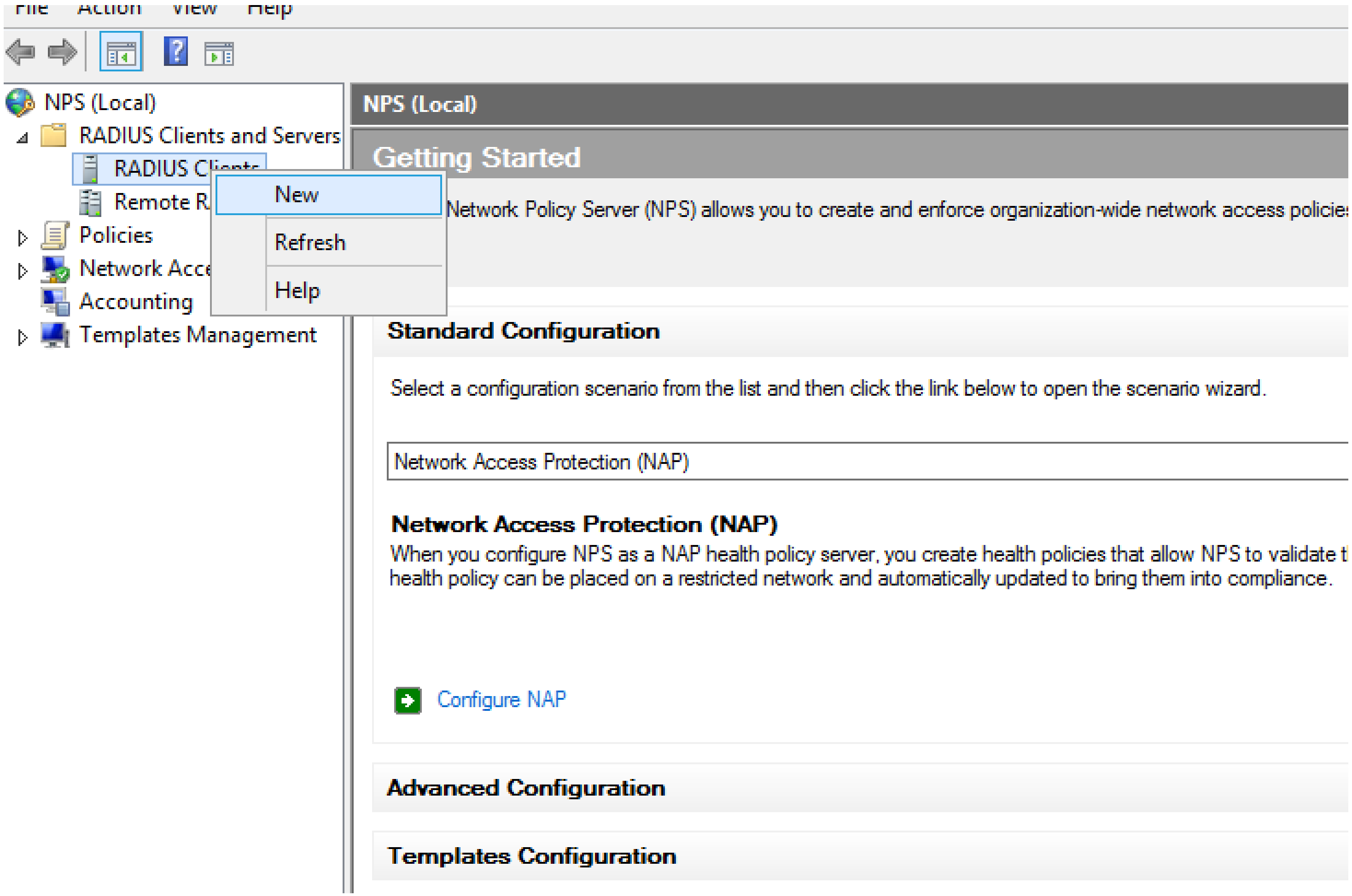
RADIUS CLIENT

Server 2012R2

Expand RADIUS Clients and Servers > (right click) Radius Clients > New



Getting Started

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policie

Standard Configuration

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

Network Access Protection (NAP)

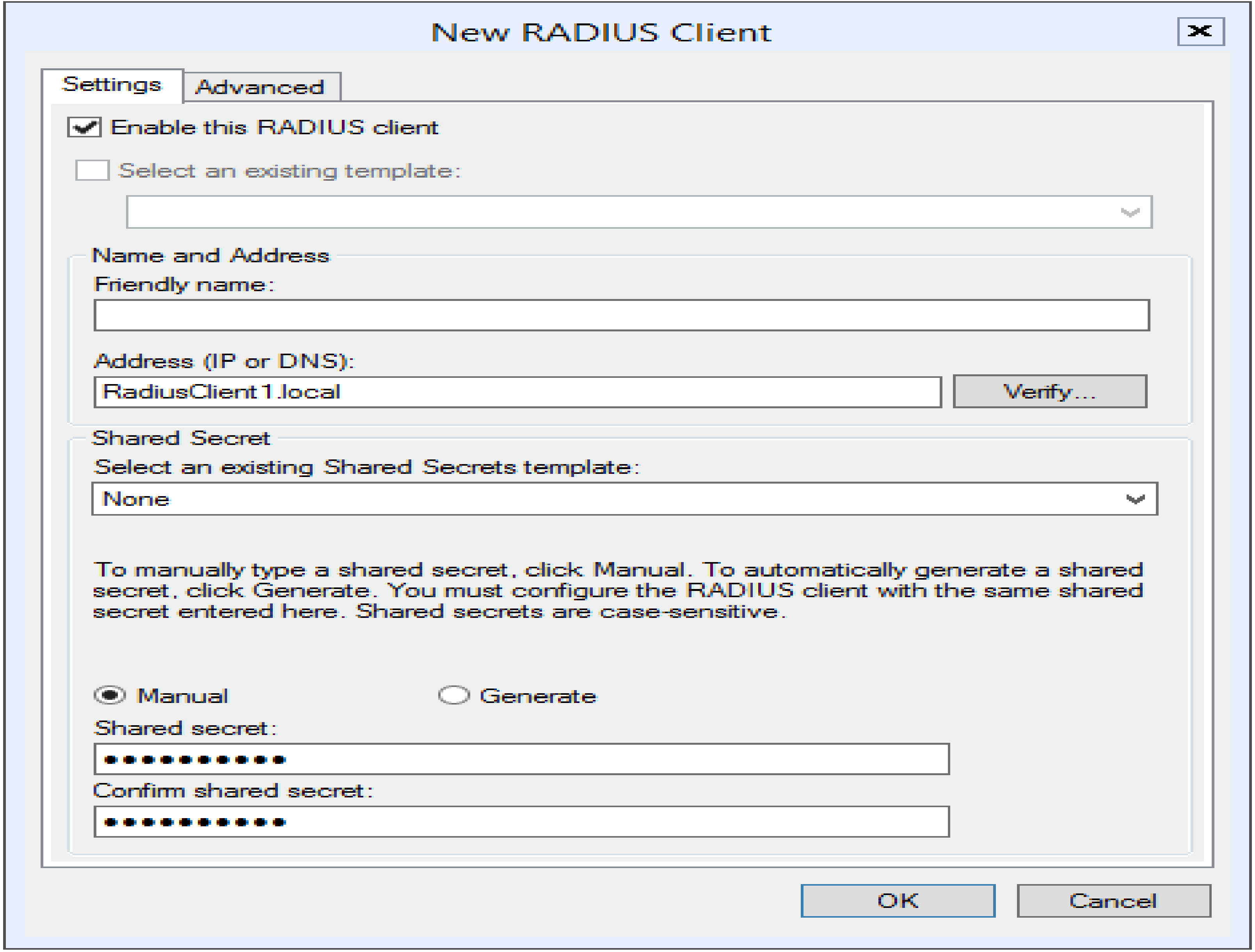
Network Access Protection (NAP)

When you configure NPS as a NAP health policy server, you create health policies that allow NPS to validate t health policy can be placed on a restricted network and automatically updated to bring them into compliance.

Configure NAP

Advanced Configuration

Templates Configuration



New RADIUS Client

Settings | Advanced

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name:

Address (IP or DNS): RadiusClient1.local

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.

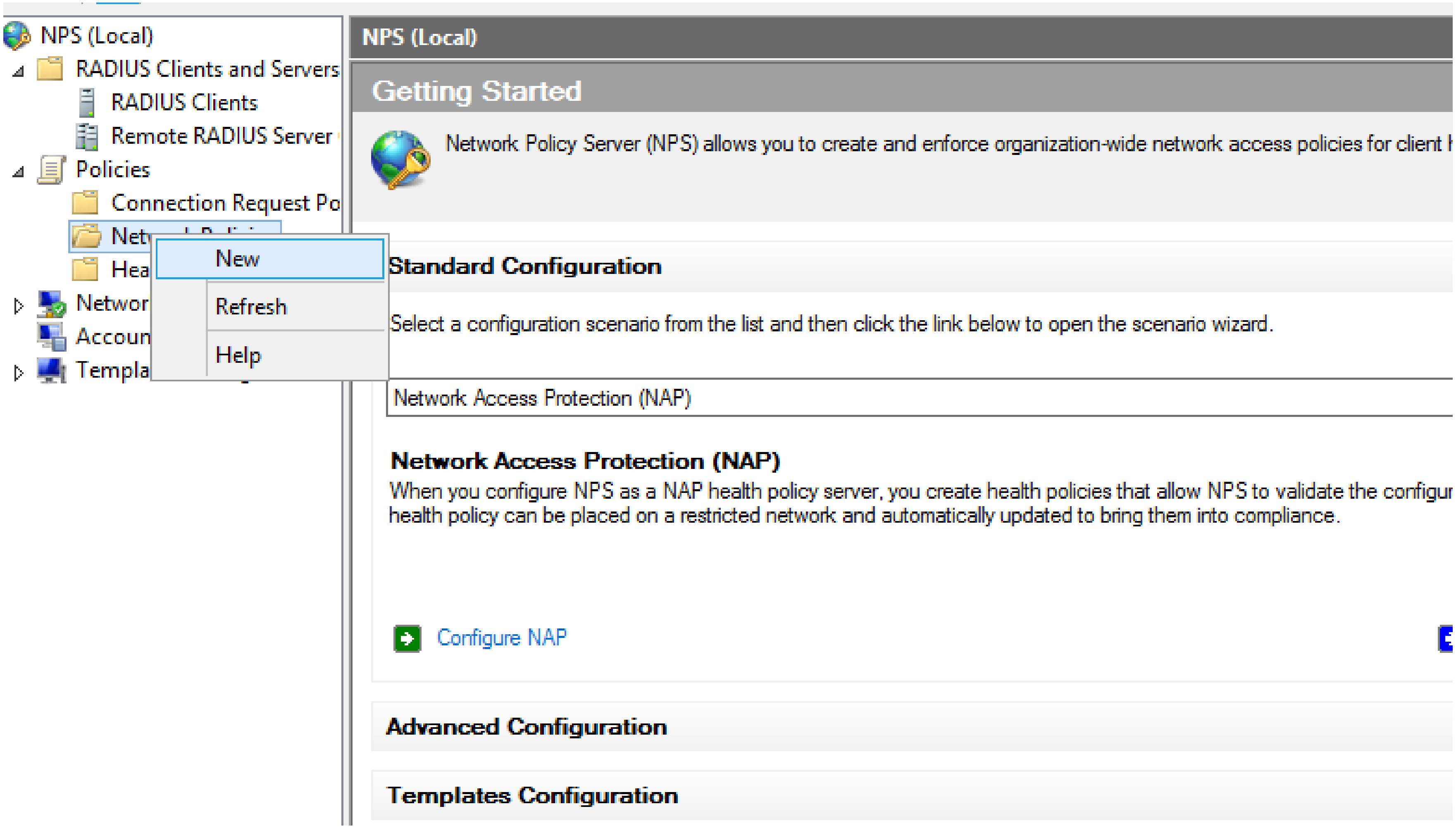
● Manual ○ Generate

Shared secret: ●●●●●●●●●●●

Confirm shared secret: ●●●●●●●●●●●

On the settings tab type the friendly name >IP of DNS of the client and enter a password, then click on OK.

Create a new Network Policy



Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client h

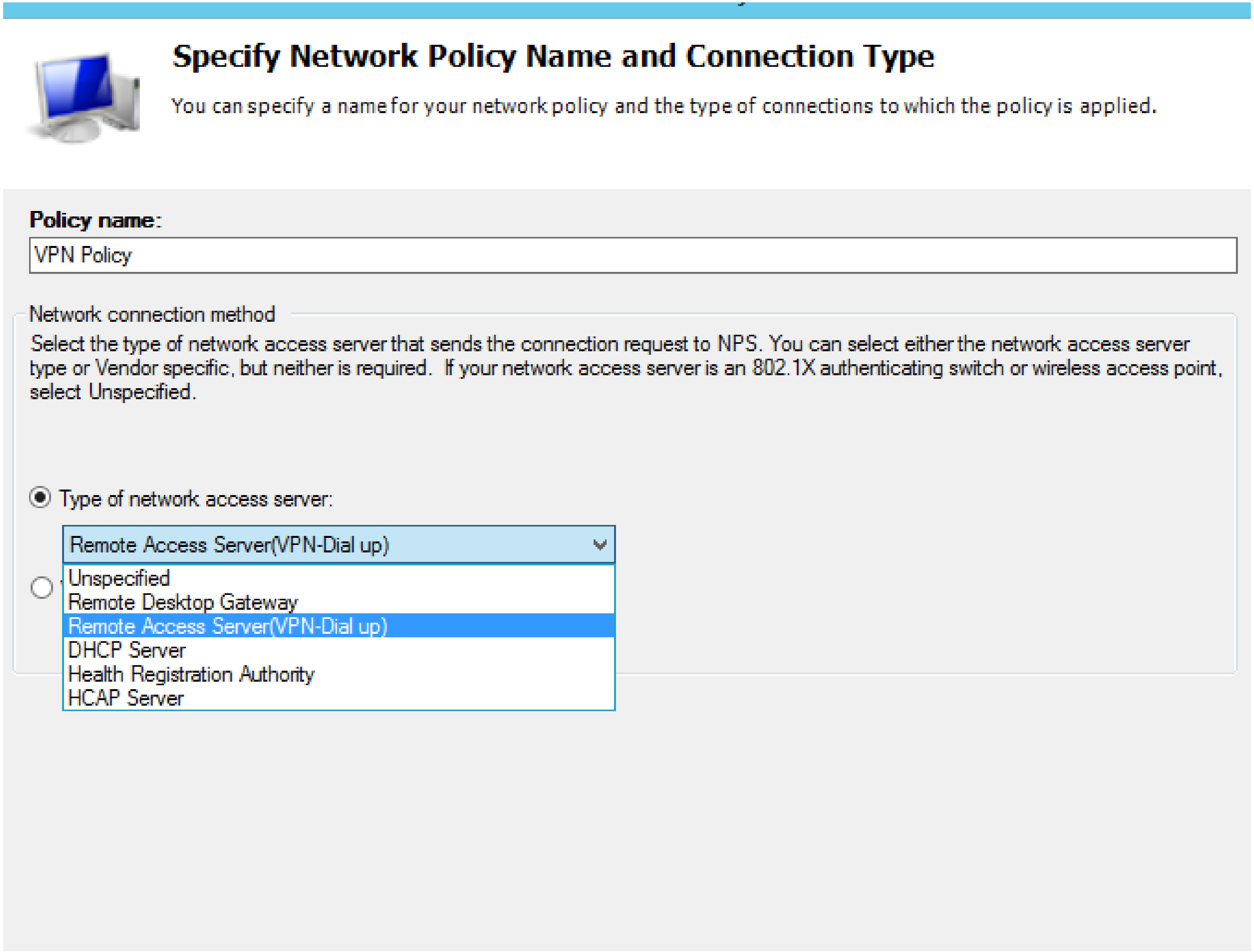
Select a configuration scenario from the list and then click the link below to open the scenario wizard.

Network Access Protection (NAP)

Network Access Protection (NAP)

When you configure NPS as a NAP health policy server, you create health policies that allow NPS to validate the configur health policy can be placed on a restricted network and automatically updated to bring them into compliance.

Expand Policies > (right click) on Network Polices > Click New



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:

VPN Policy

Network connection method

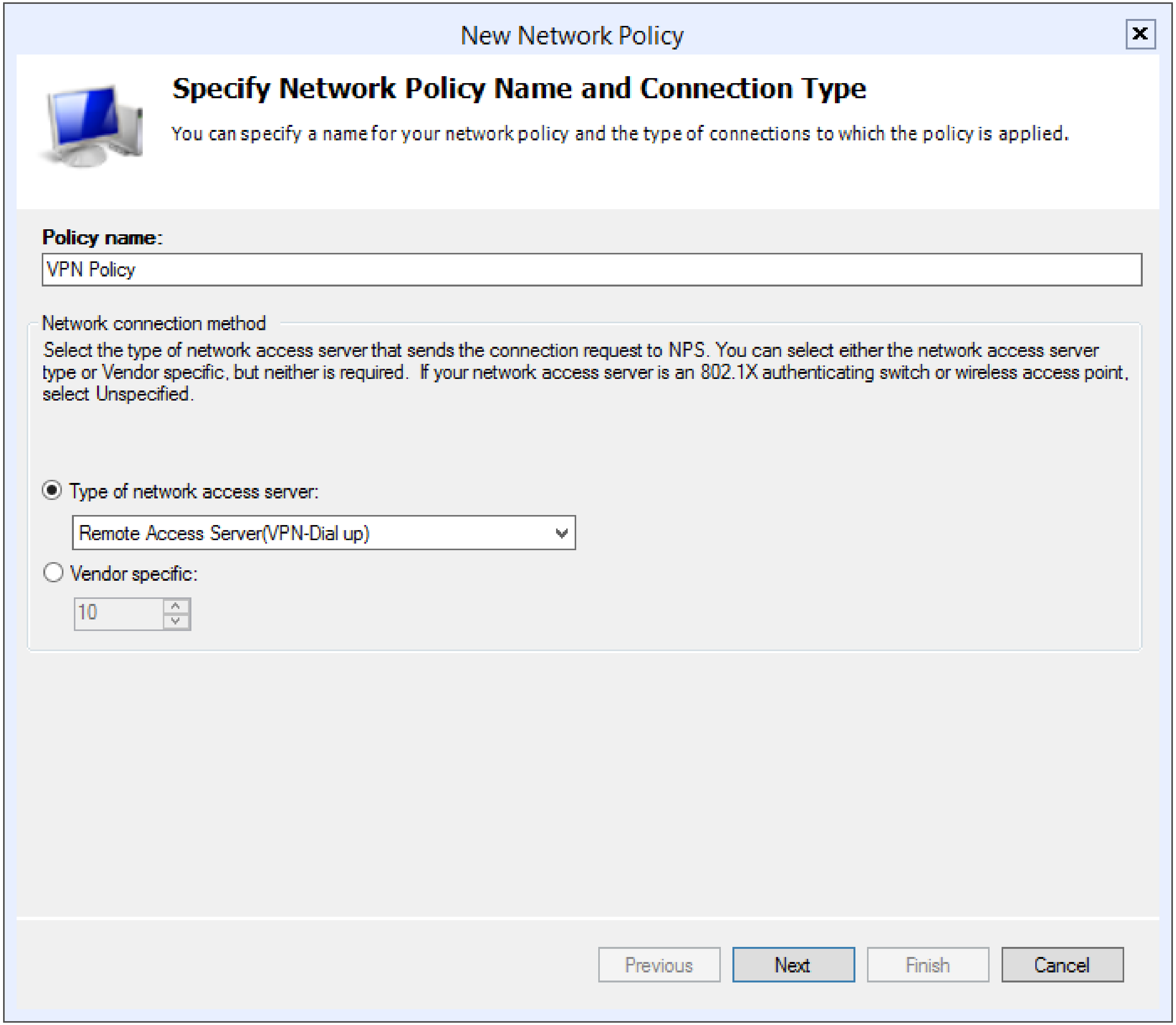
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

● Type of network access server:

Remote Access Server(VPN-Dial up)

- Unspecified
- Remote Desktop Gateway
- Remote Access Server(VPN-Dial up)
- DHCP Server
- Health Registration Authority
- HCAP Server

○



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:

VPN Policy

Network connection method

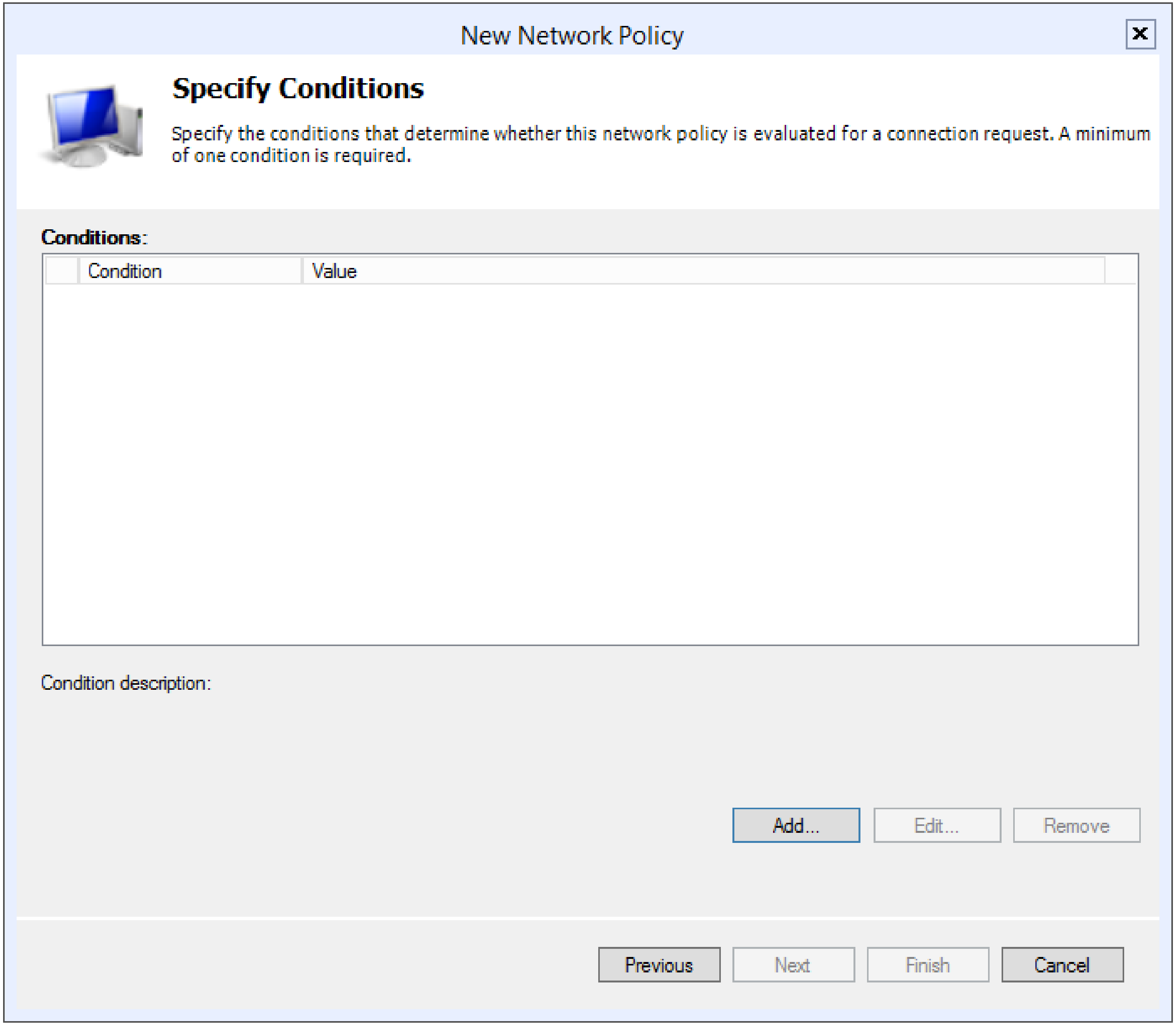
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

● Type of network access server:

Remote Access Server(VPN-Dial up)

○ Vendor specific:

10



New Network Policy

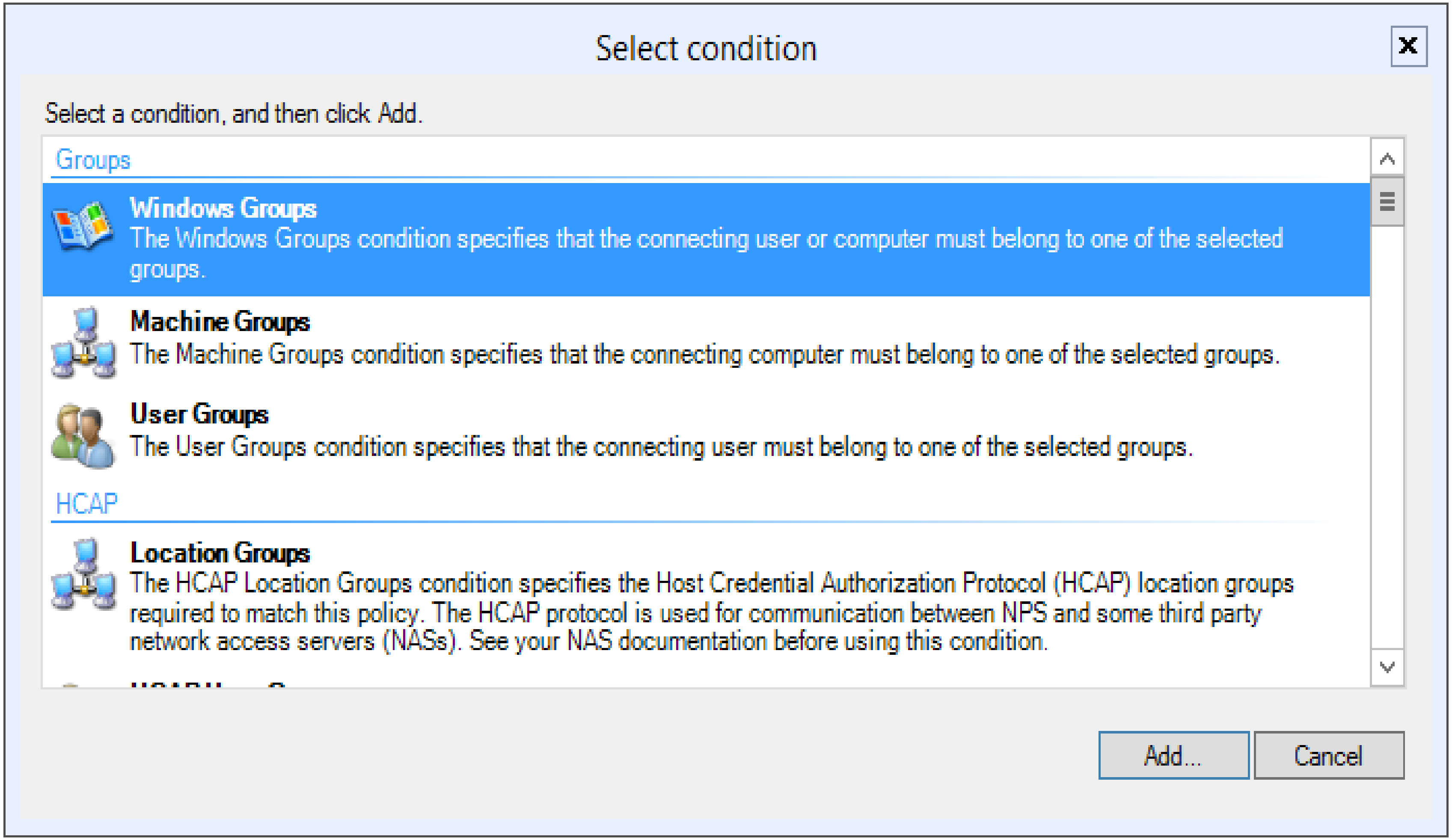
Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value

Condition description:



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.

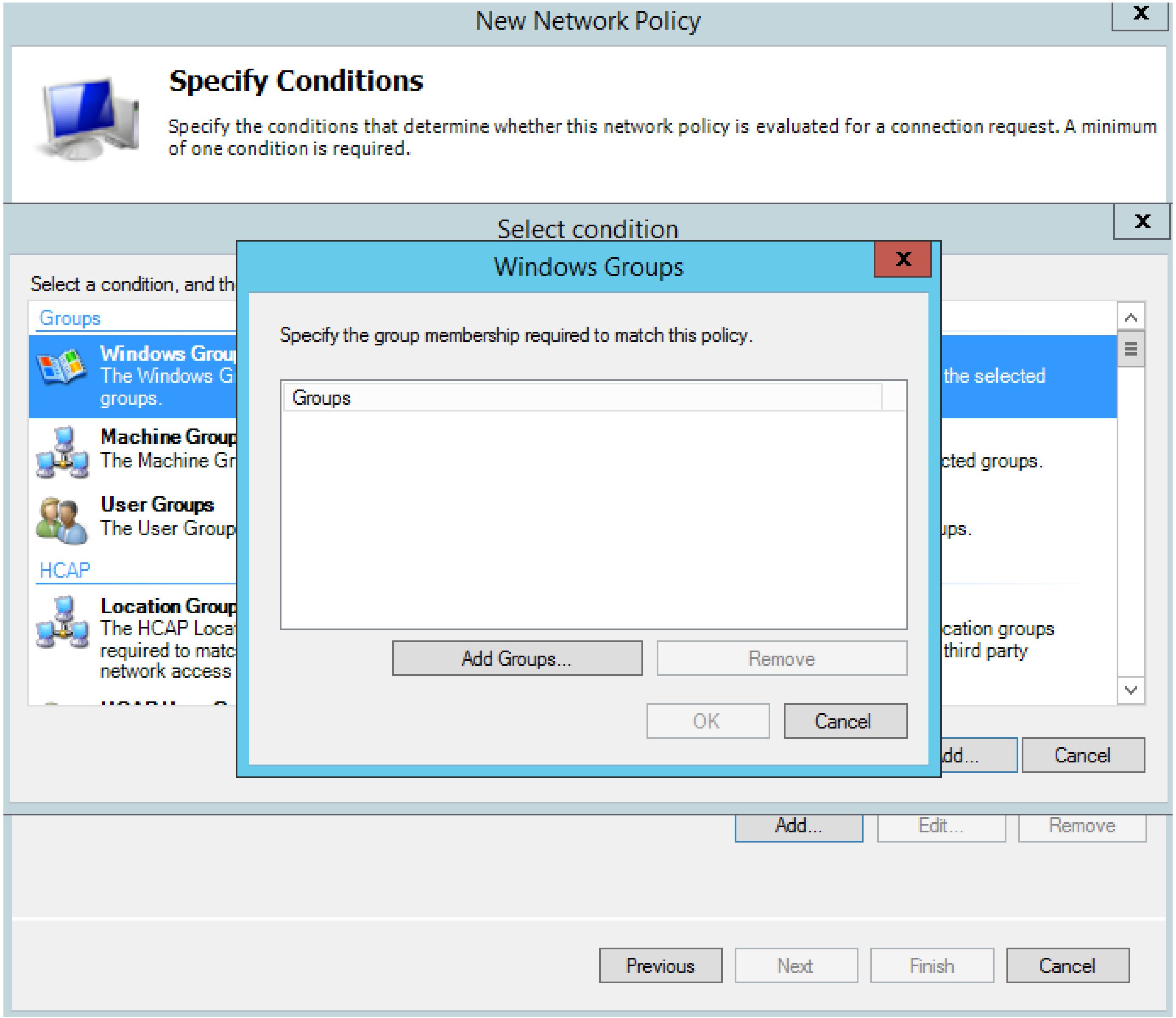
Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

HCAP

Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

Select the Windows Groups, then click Add



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.

Select condition

Select a condition, and th

Groups

Windows Grou
The Windows G ... the selected groups.

Machine Group
The Machine Gr ... cted groups.

User Groups
The User Group ... ups.

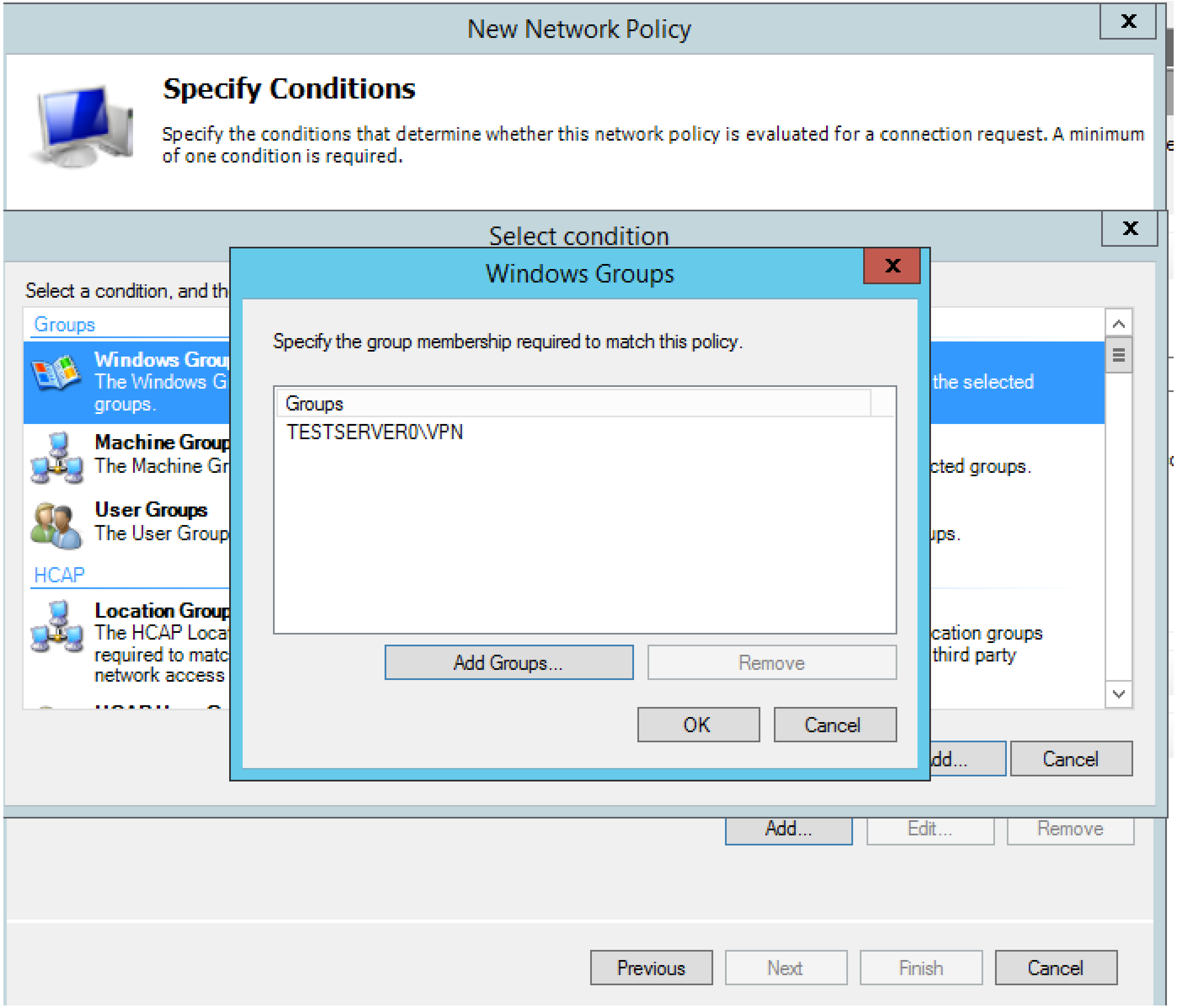
HCAP

Location Group
The HCAP Loca ... cation groups required to matc ... third party network access

Windows Groups

Specify the group membership required to match this policy.

Groups



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.

Select condition

Select a condition, and th

Groups

Windows Grou The Windows G groups. the selected

Machine Group The Machine Gr cted groups.

User Groups The User Group ups.

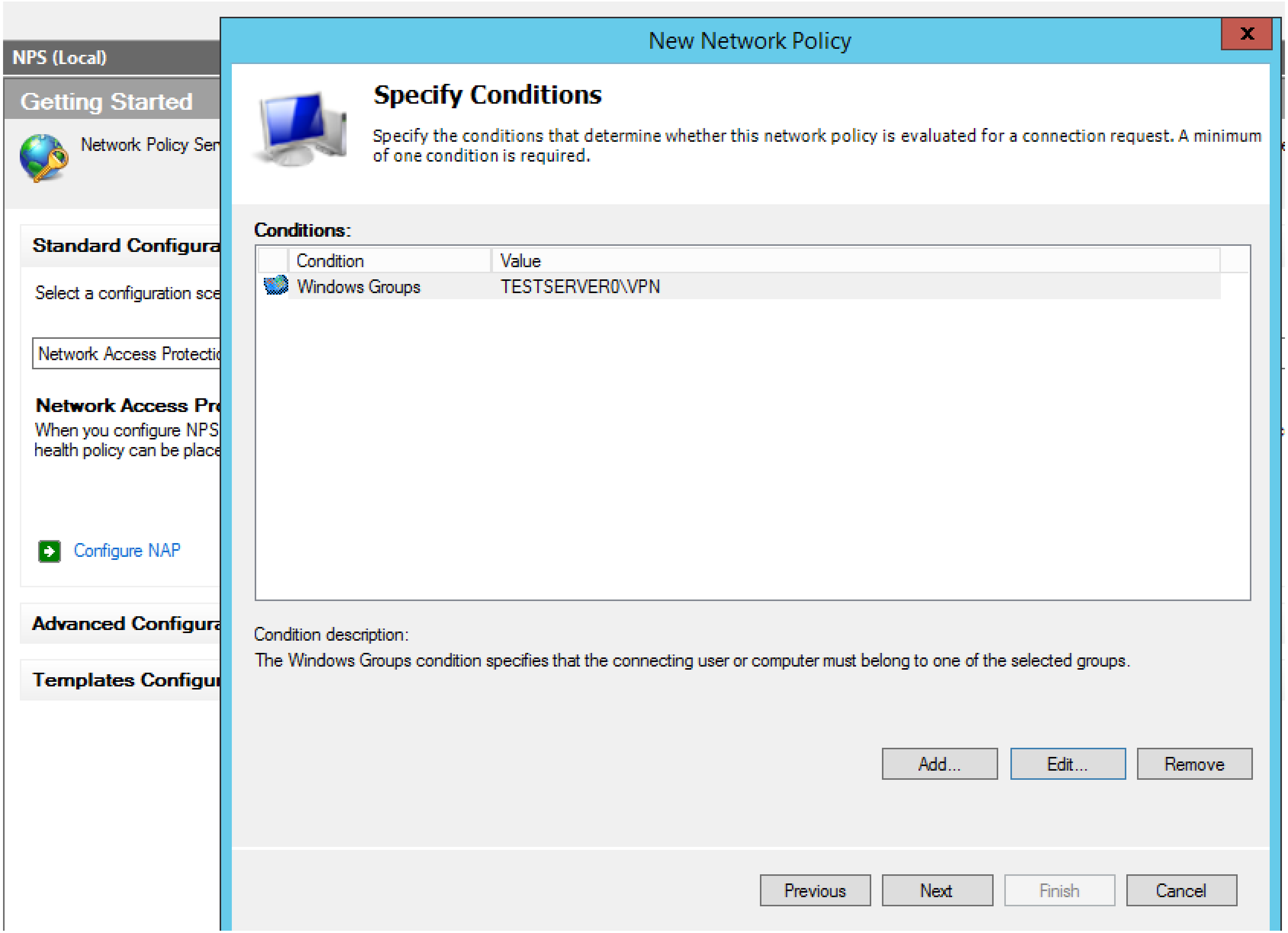
HCAP

Location Group The HCAP Locat required to matc network access cation groups third party

Windows Groups

Specify the group membership required to match this policy.

Groups
TESTSERVER0\VPN



Specify Conditions

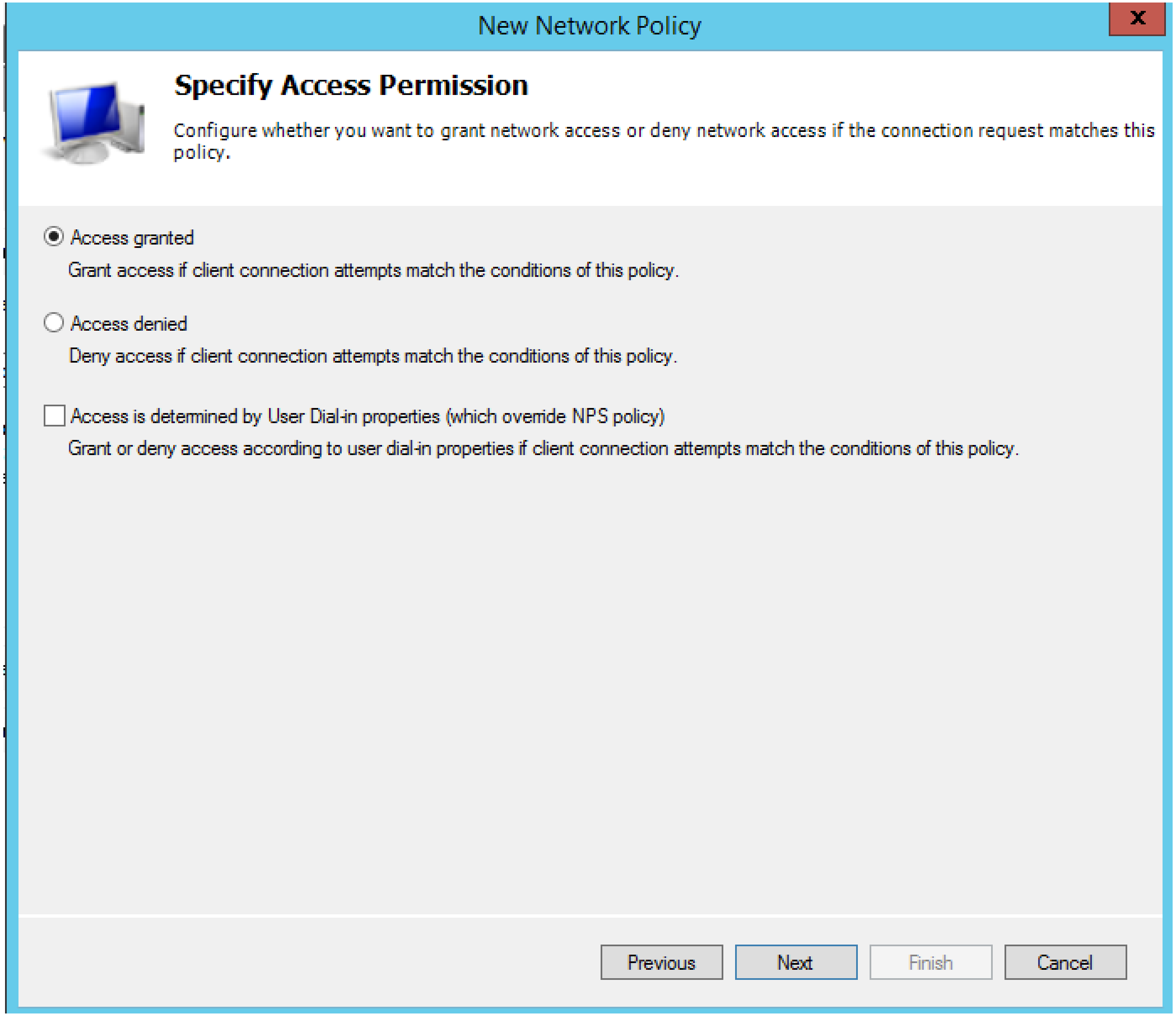
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
Windows Groups	TESTSERVER0\VPN

Condition description:

The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected 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

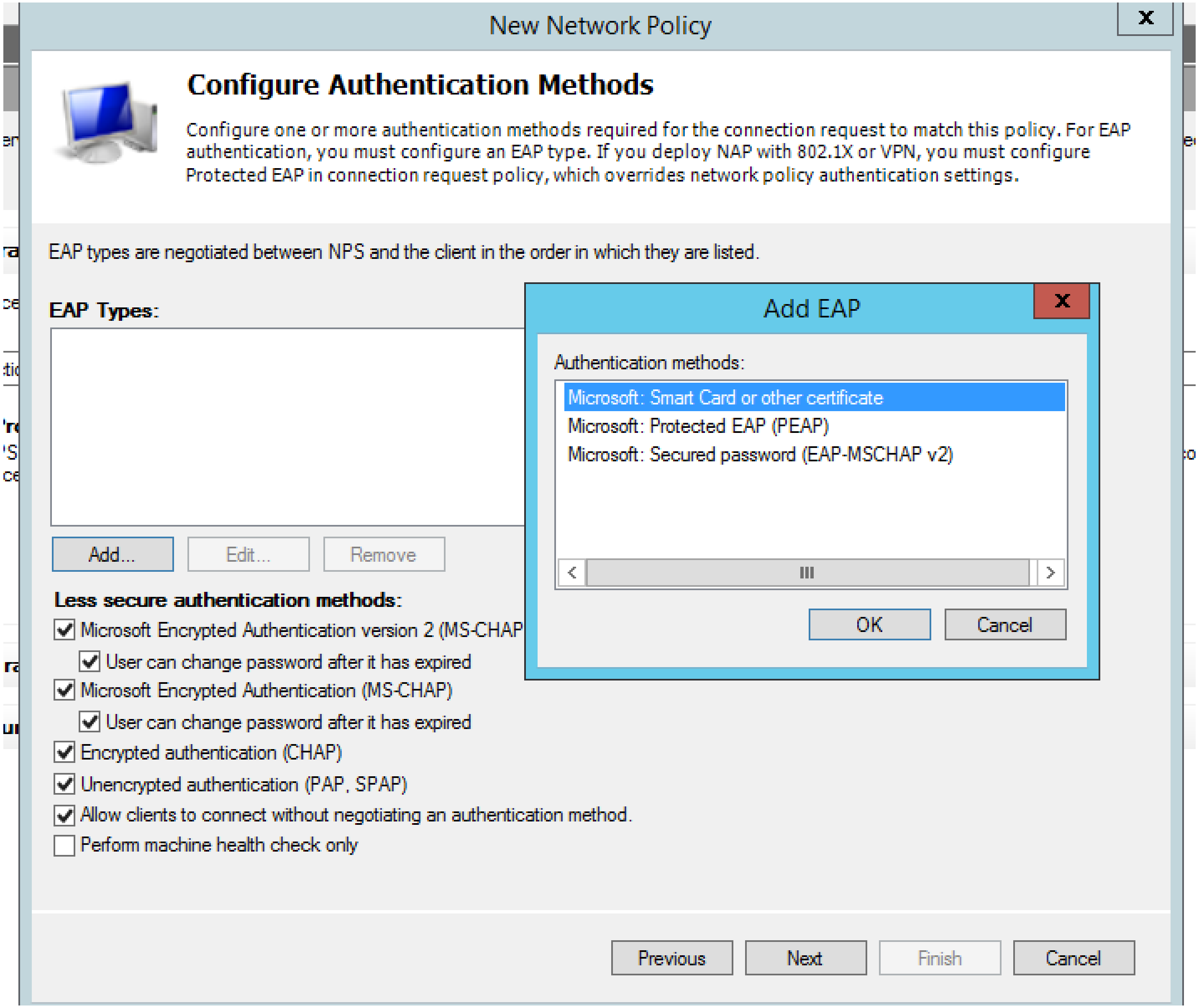
Grant access if client connection attempts match the conditions of this policy.

○ 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.



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. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

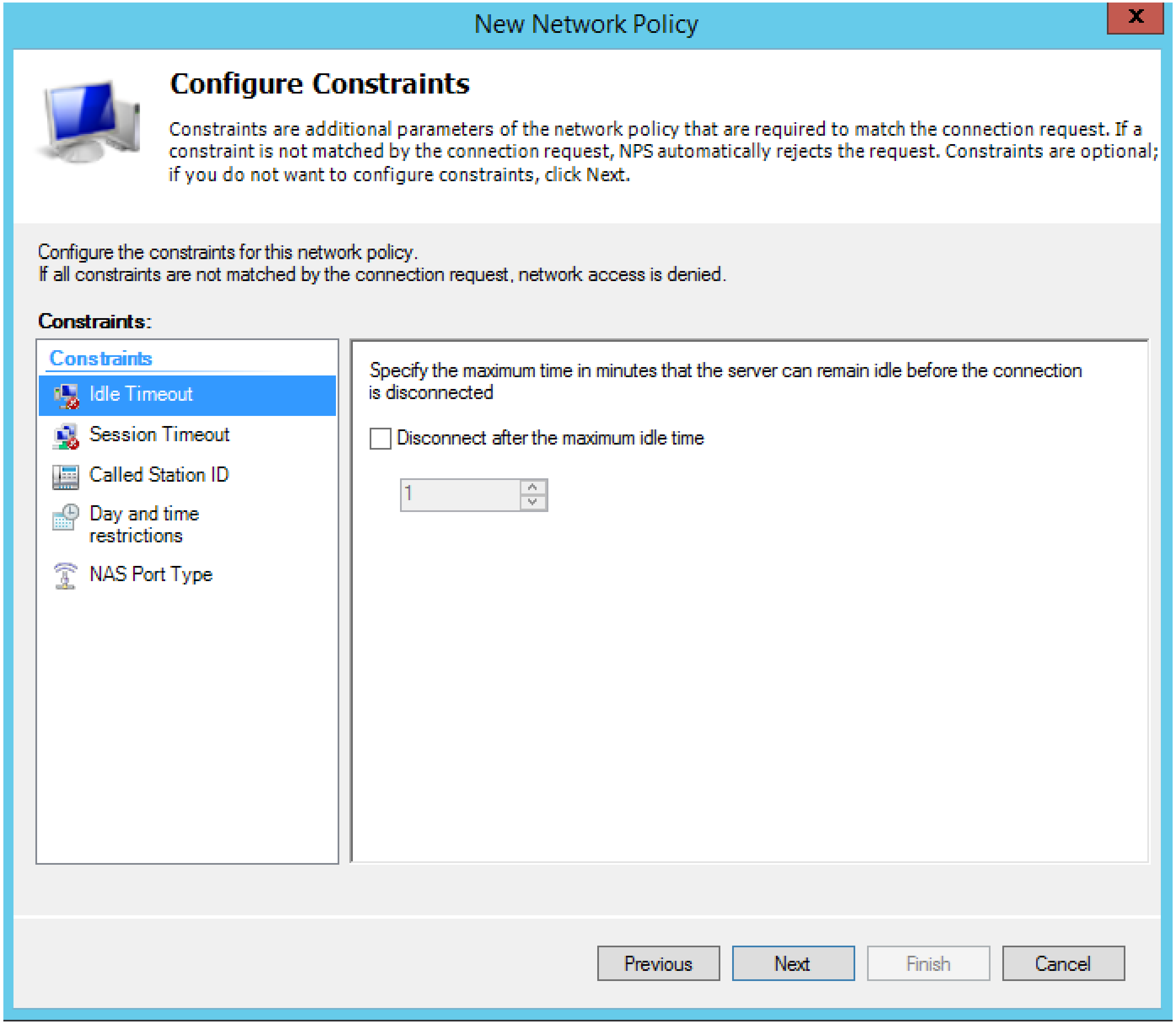
EAP Types:

Less secure authentication methods:

- ☑ Microsoft Encrypted Authentication version 2 (MS-CHAP
  - ☑ 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.
- □ Perform machine health check only

Authentication methods:

- Microsoft: Smart Card or other certificate
- Microsoft: Protected EAP (PEAP)
- Microsoft: Secured password (EAP-MSCHAP v2)



New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

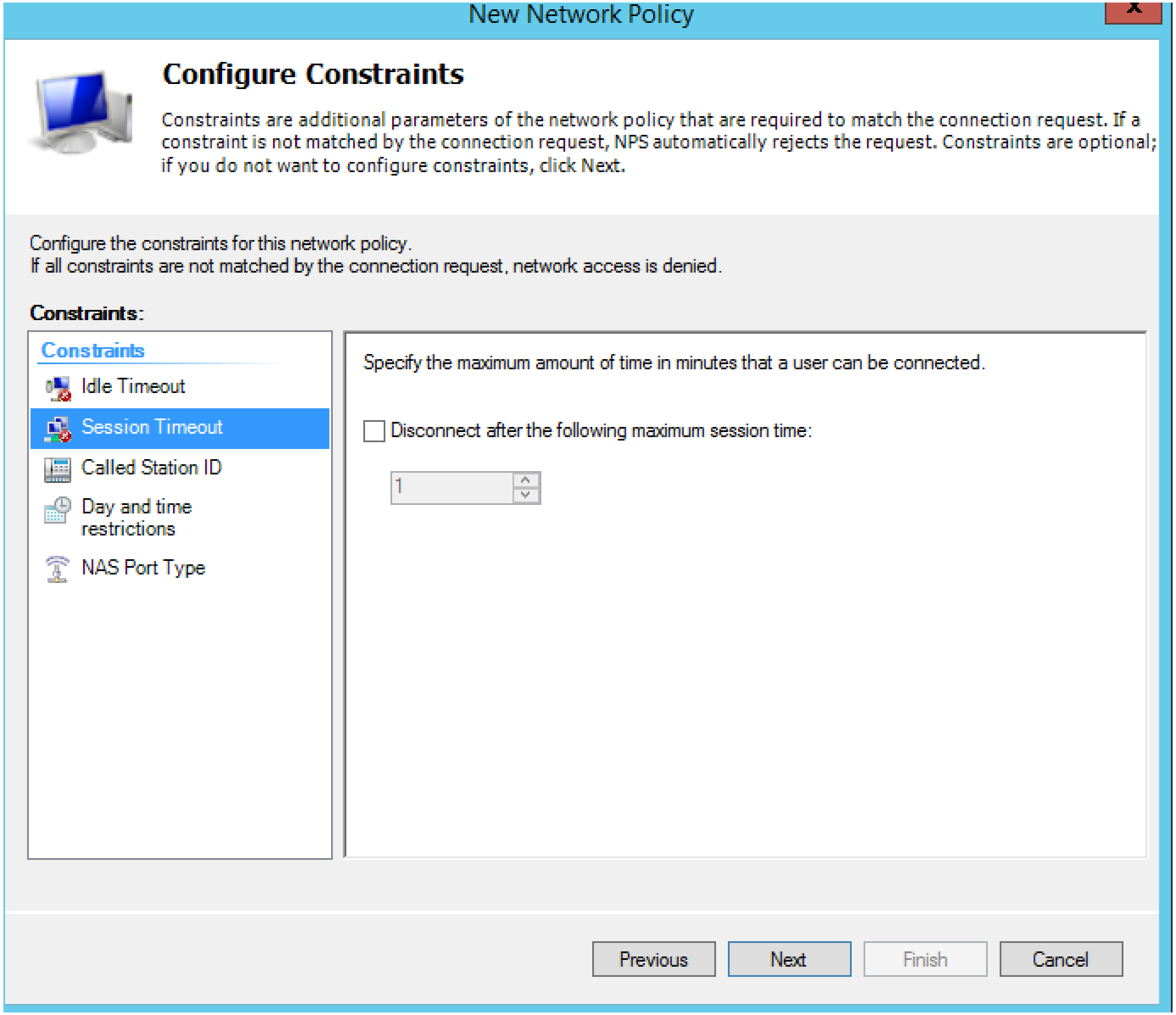
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

1



New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

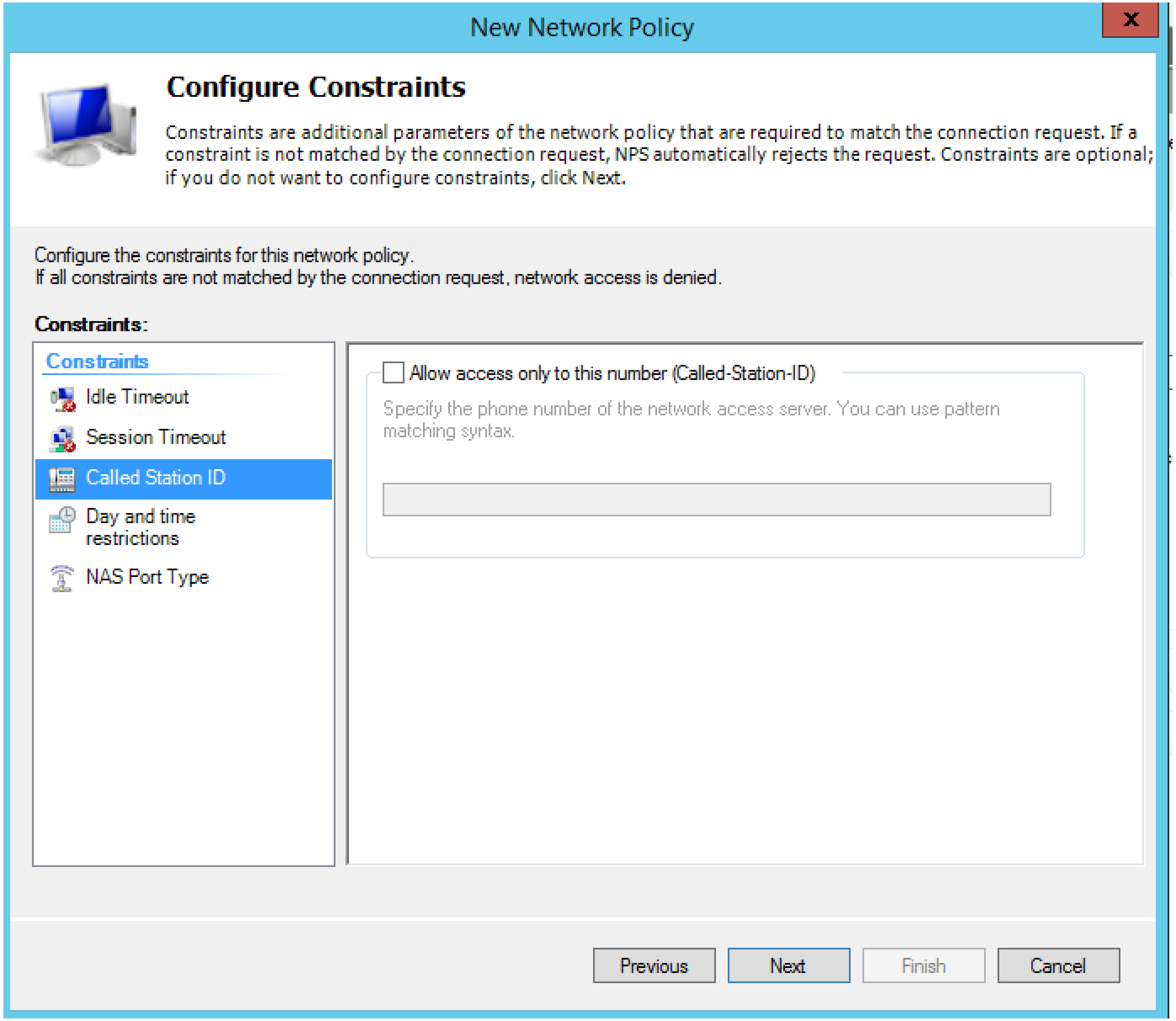
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Specify the maximum amount of time in minutes that a user can be connected.

□ Disconnect after the following maximum session time:

1



New Network Policy

Configure Constraints

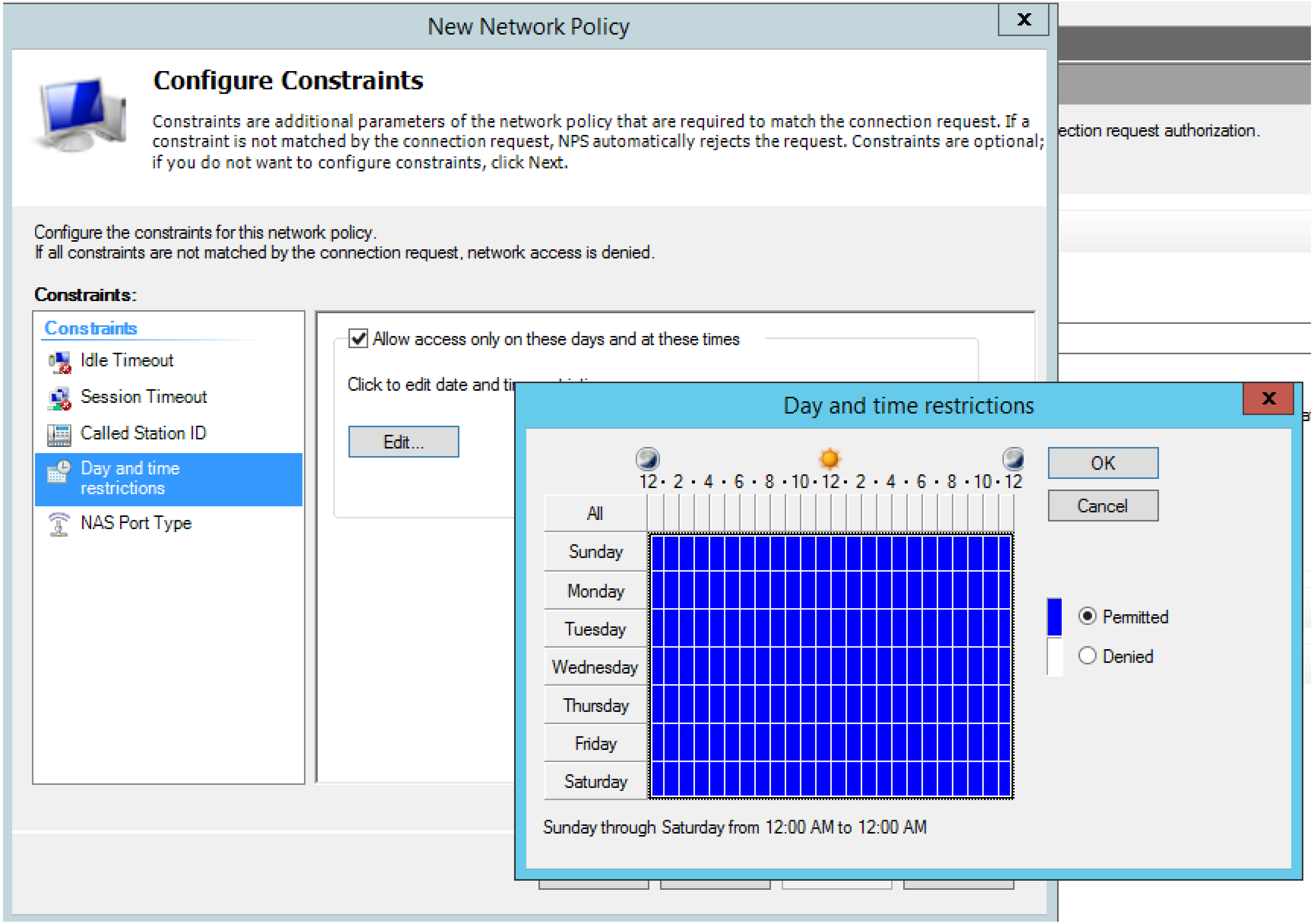
Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

□ Allow access only to this number (Called-Station-ID)

Specify the phone number of the network access server. You can use pattern matching syntax.



New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

ection request authorization.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

☑ Allow access only on these days and at these times

Click to edit date and ti

Edit...

Day and time restrictions

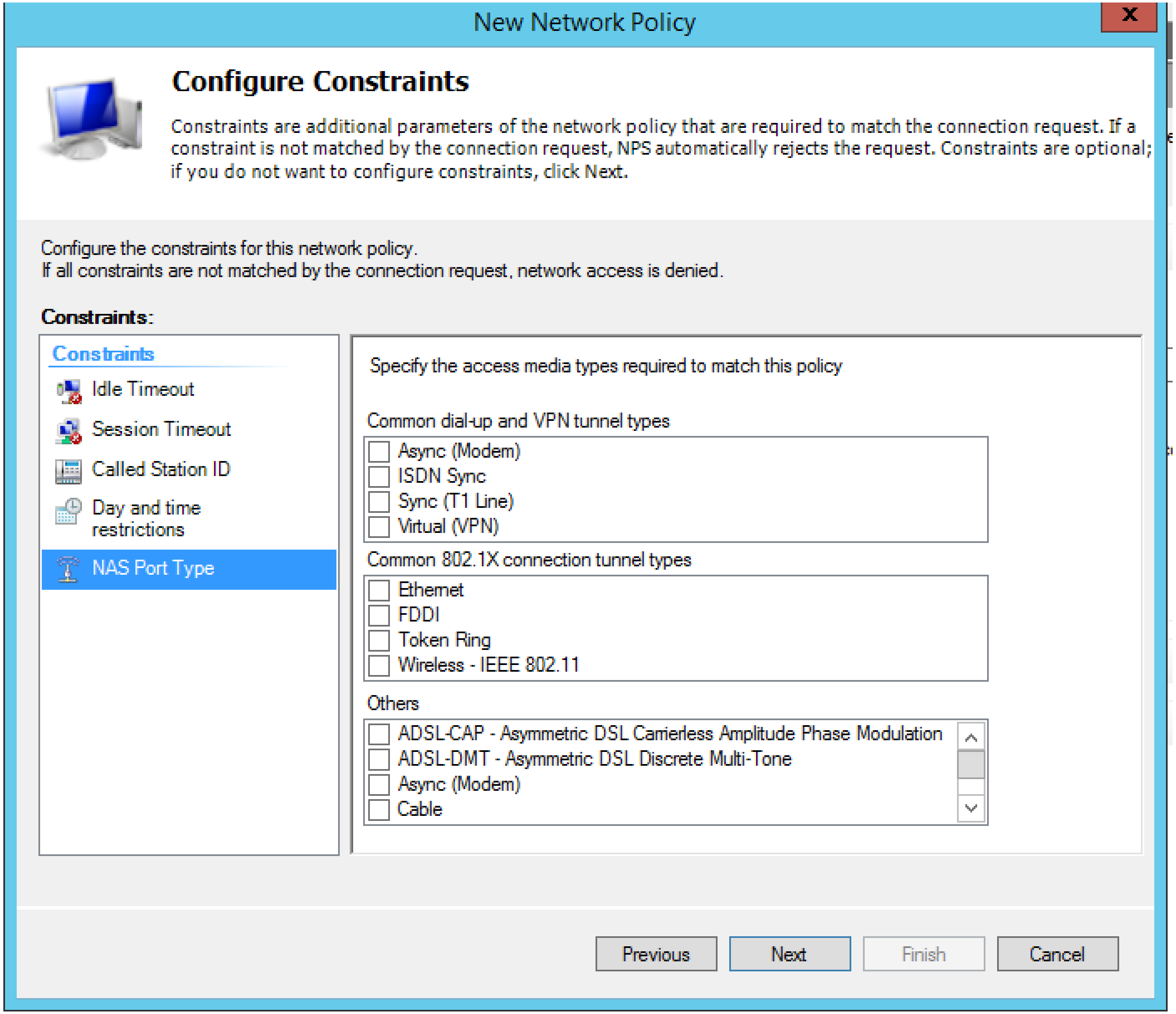
12 · 2 · 4 · 6 · 8 · 10 · 12 · 2 · 4 · 6 · 8 · 10 · 12

All
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday

OK
Cancel

● Permitted
○ Denied

Sunday through Saturday from 12:00 AM to 12:00 AM



New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

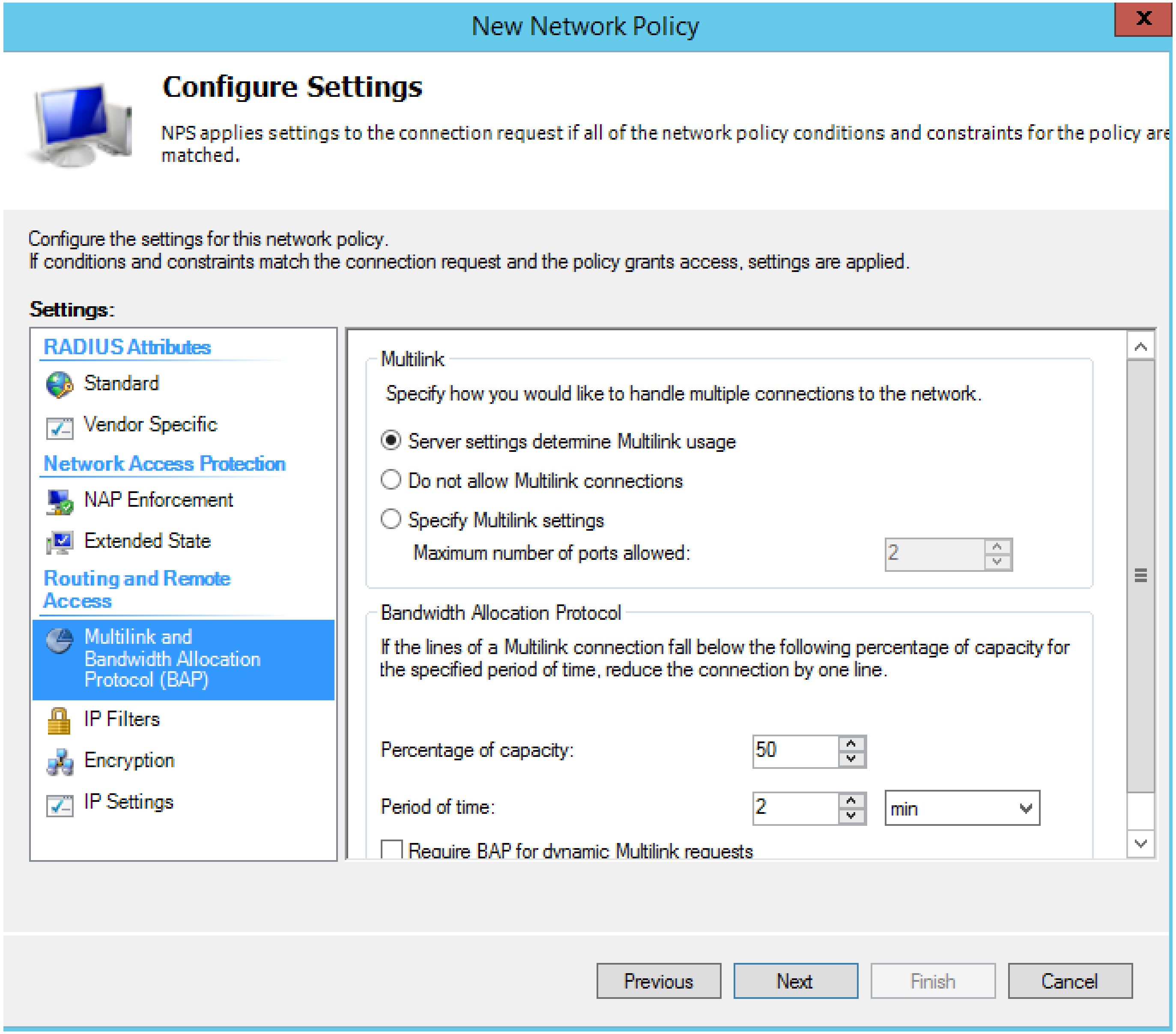
Constraints
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Specify the access media types required to match this policy

Common dial-up and VPN tunnel types
- □ Async (Modem)
- □ ISDN Sync
- □ Sync (T1 Line)
- □ Virtual (VPN)

Common 802.1X connection tunnel types
- □ Ethernet
- □ FDDI
- □ Token Ring
- □ Wireless - IEEE 802.11

Others
- □ ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation
- □ ADSL-DMT - Asymmetric DSL Discrete Multi-Tone
- □ Async (Modem)
- □ Cable



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 for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

Multilink

Specify how you would like to handle multiple connections to the network.

● Server settings determine Multilink usage

○ Do not allow Multilink connections

○ Specify Multilink settings

Maximum number of ports allowed: 2

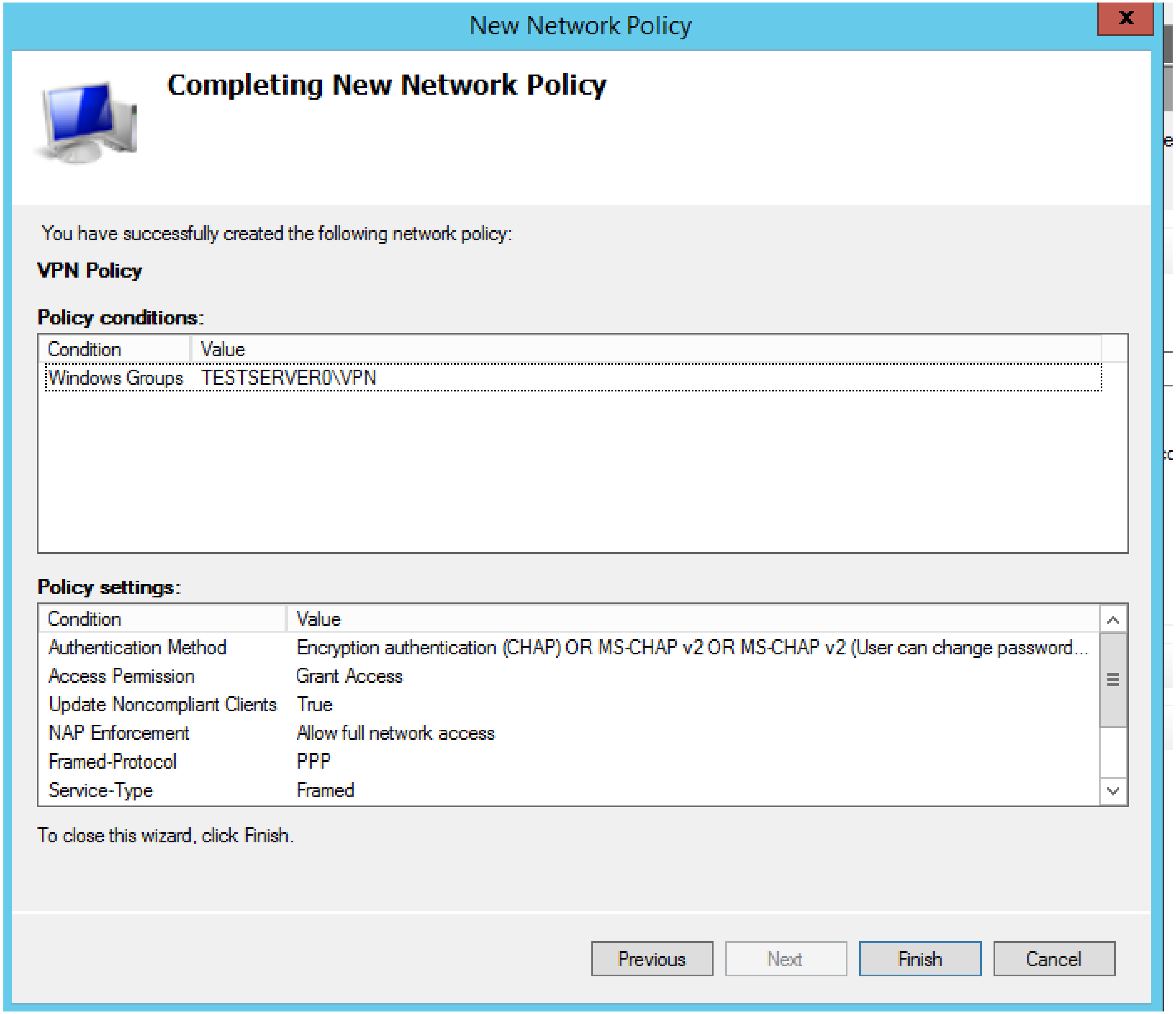
Bandwidth Allocation Protocol

If the lines of a Multilink connection fall below the following percentage of capacity for the specified period of time, reduce the connection by one line.

Percentage of capacity: 50

Period of time: 2 min

□ Require BAP for dynamic Multilink requests



New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

VPN Policy

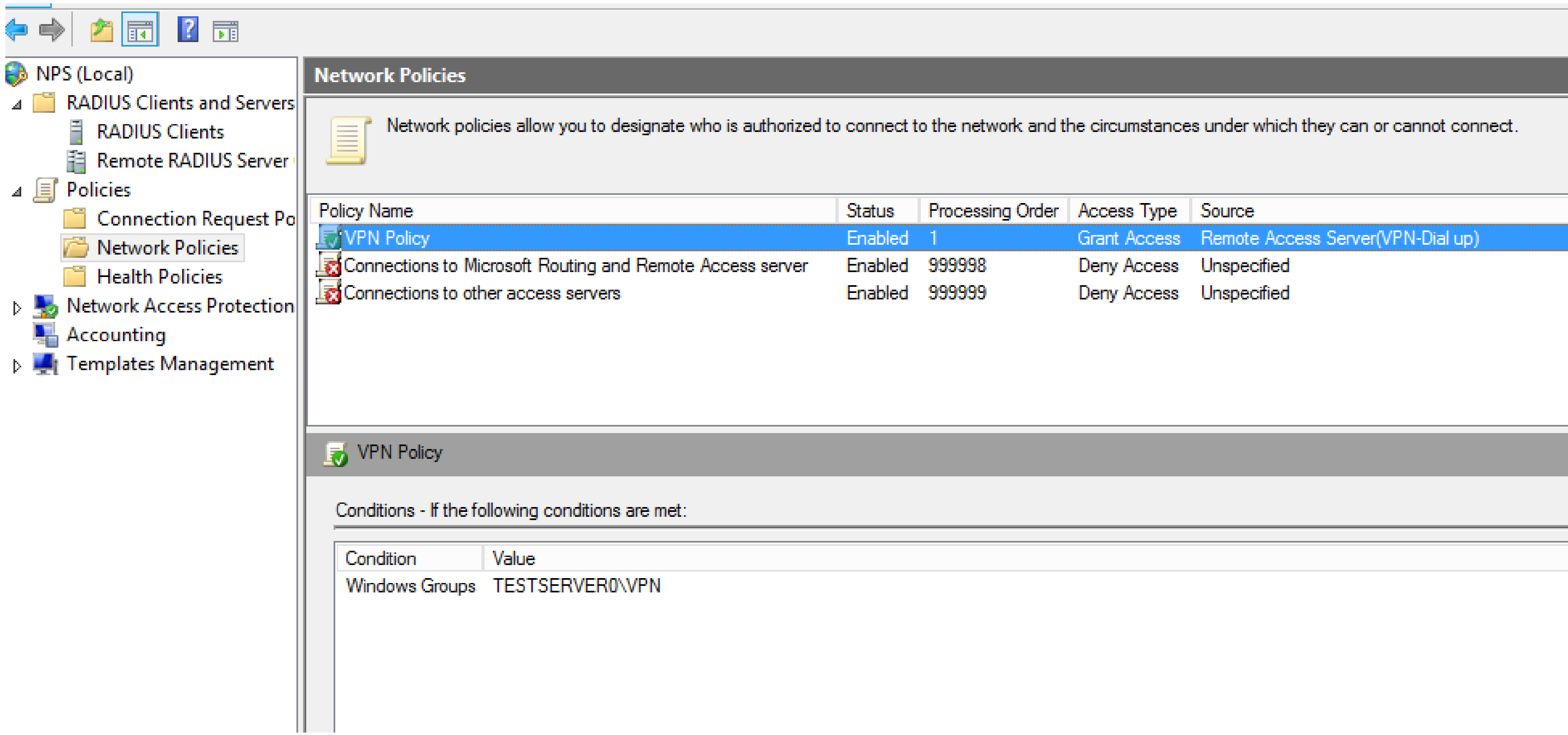
Policy conditions:

Condition	Value
Windows Groups	TESTSERVER0\VPN

Policy settings:

Condition	Value
Authentication Method	Encryption authentication (CHAP) OR MS-CHAP v2 OR MS-CHAP v2 (User can change password...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.



Network Policies

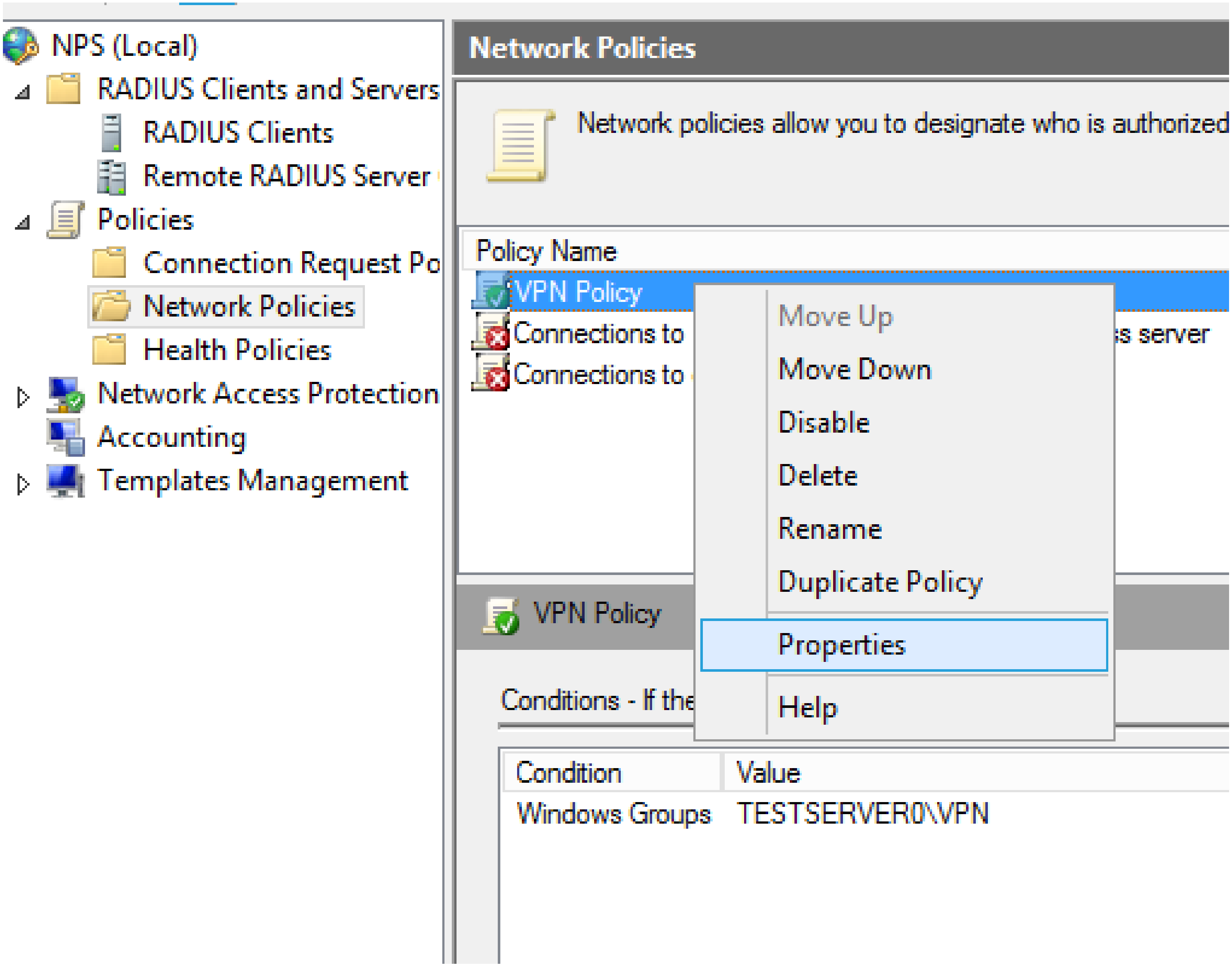
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
VPN Policy	Enabled	1	Grant Access	Remote Access Server(VPN-Dial up)
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
Connections to other access servers	Enabled	999999	Deny Access	Unspecified

VPN Policy

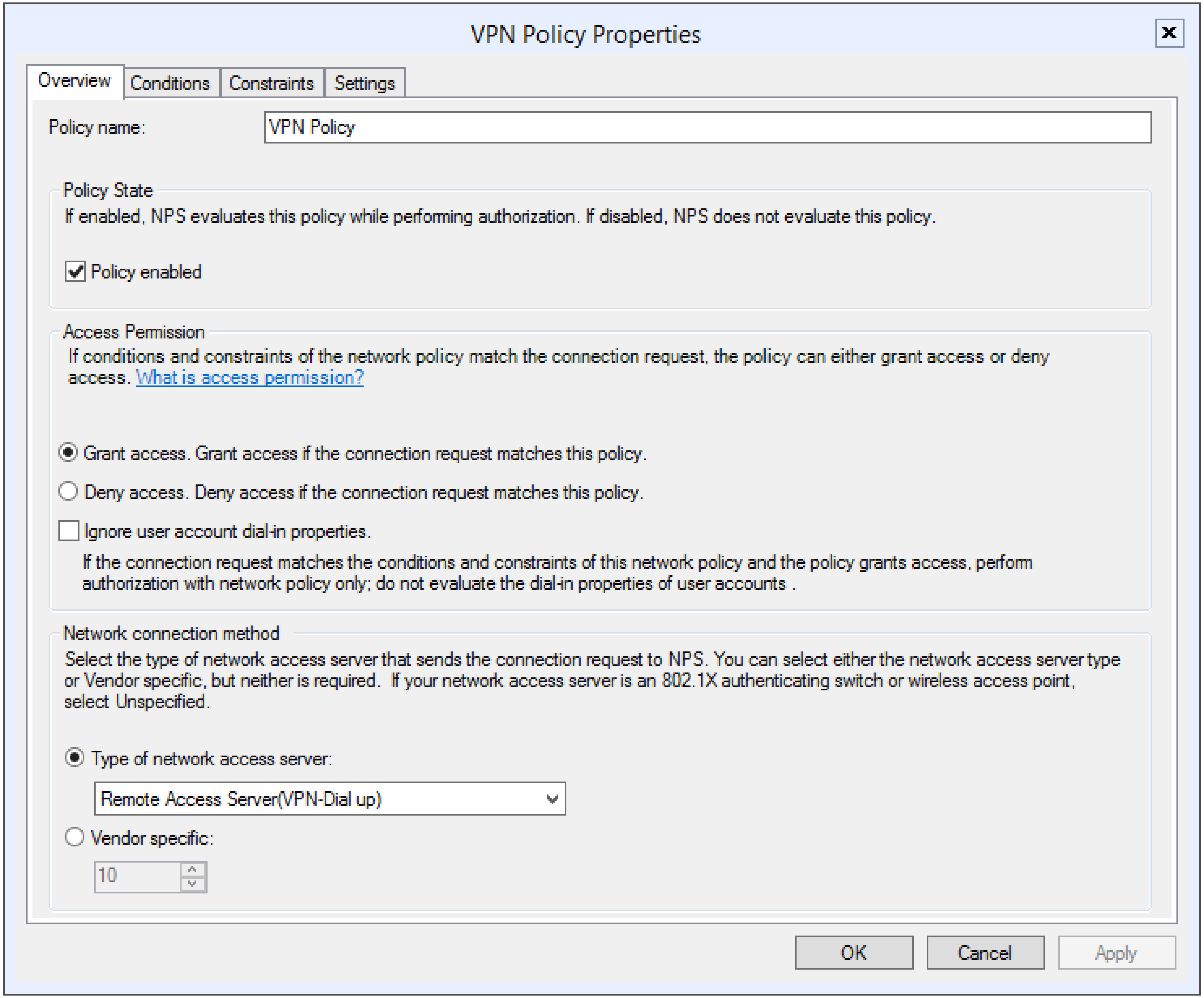
Conditions - If the following conditions are met:

Condition	Value
Windows Groups	TESTSERVER0\VPN



Network policies allow you to designate who is authorized

Condition	Value
Windows Groups	TESTSERVER0\VPN



VPN Policy Properties

Policy name: VPN Policy

Policy State

If enabled, NPS evaluates this policy while perfoming 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

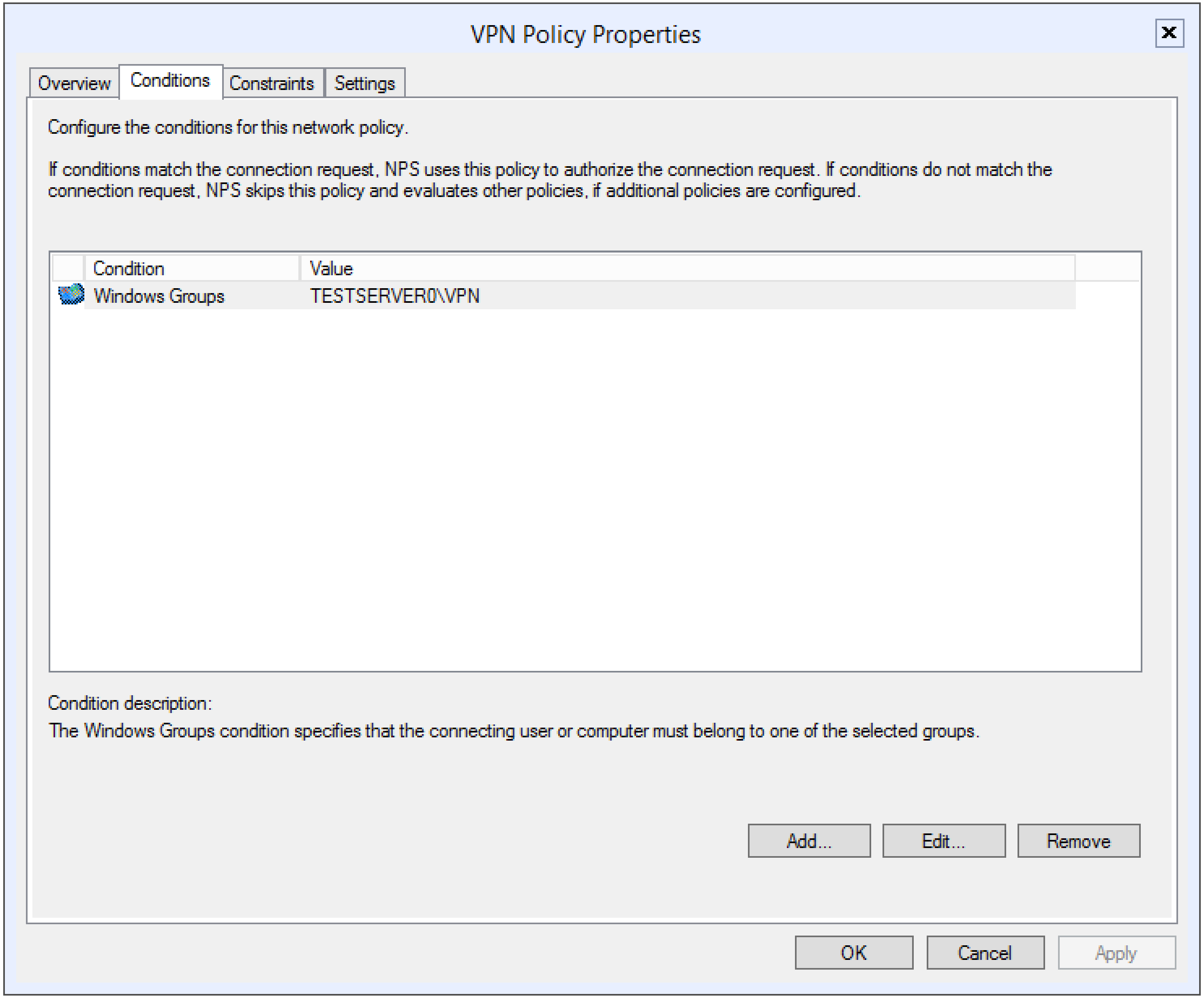
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

● Type of network access server:

Remote Access Server(VPN-Dial up)

○ Vendor specific:

10



VPN Policy Properties

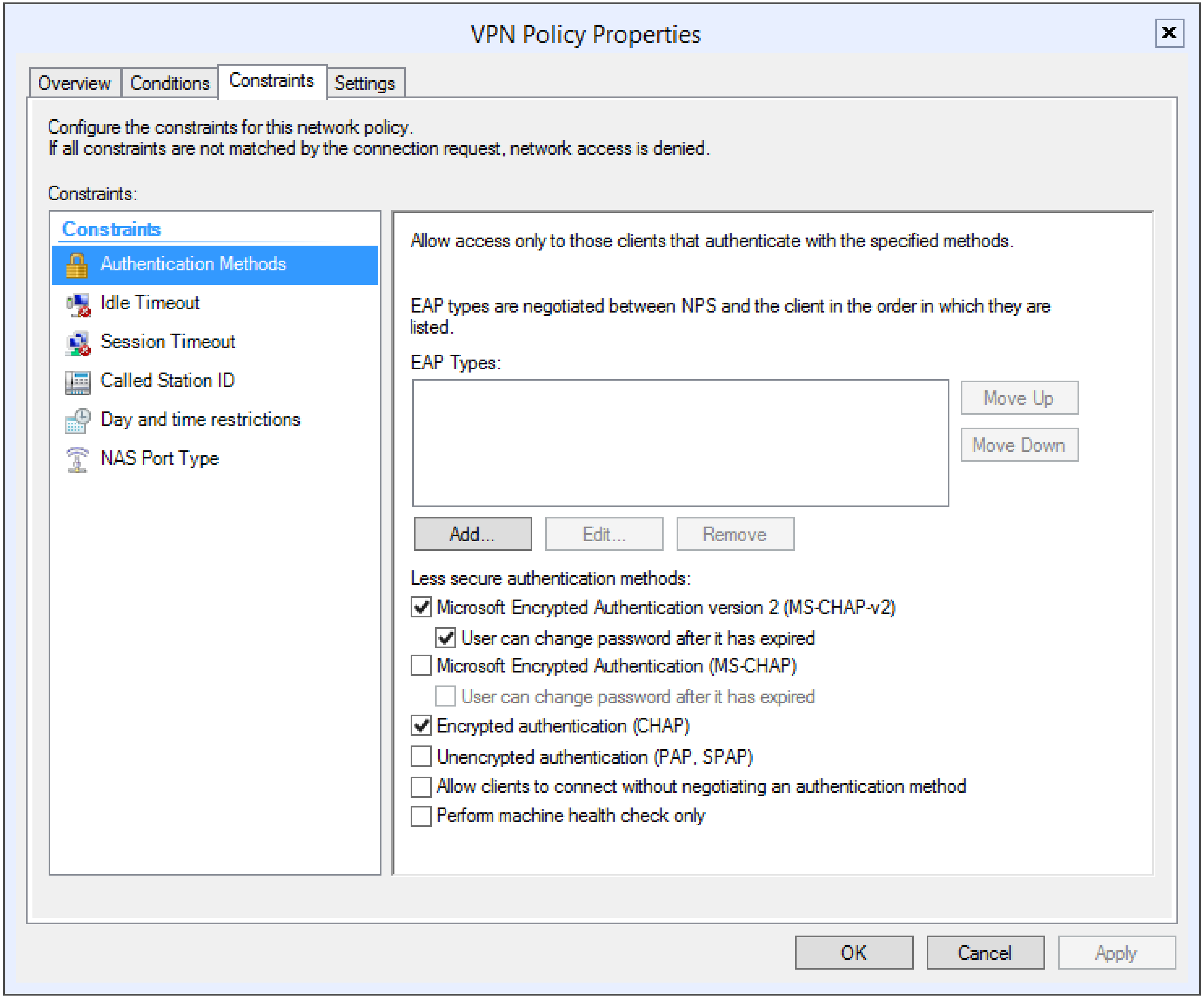
Configure the conditions for this network policy.

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
Windows Groups	TESTSERVER0\VPN

Condition description:

The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.



VPN Policy Properties

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

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:

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)

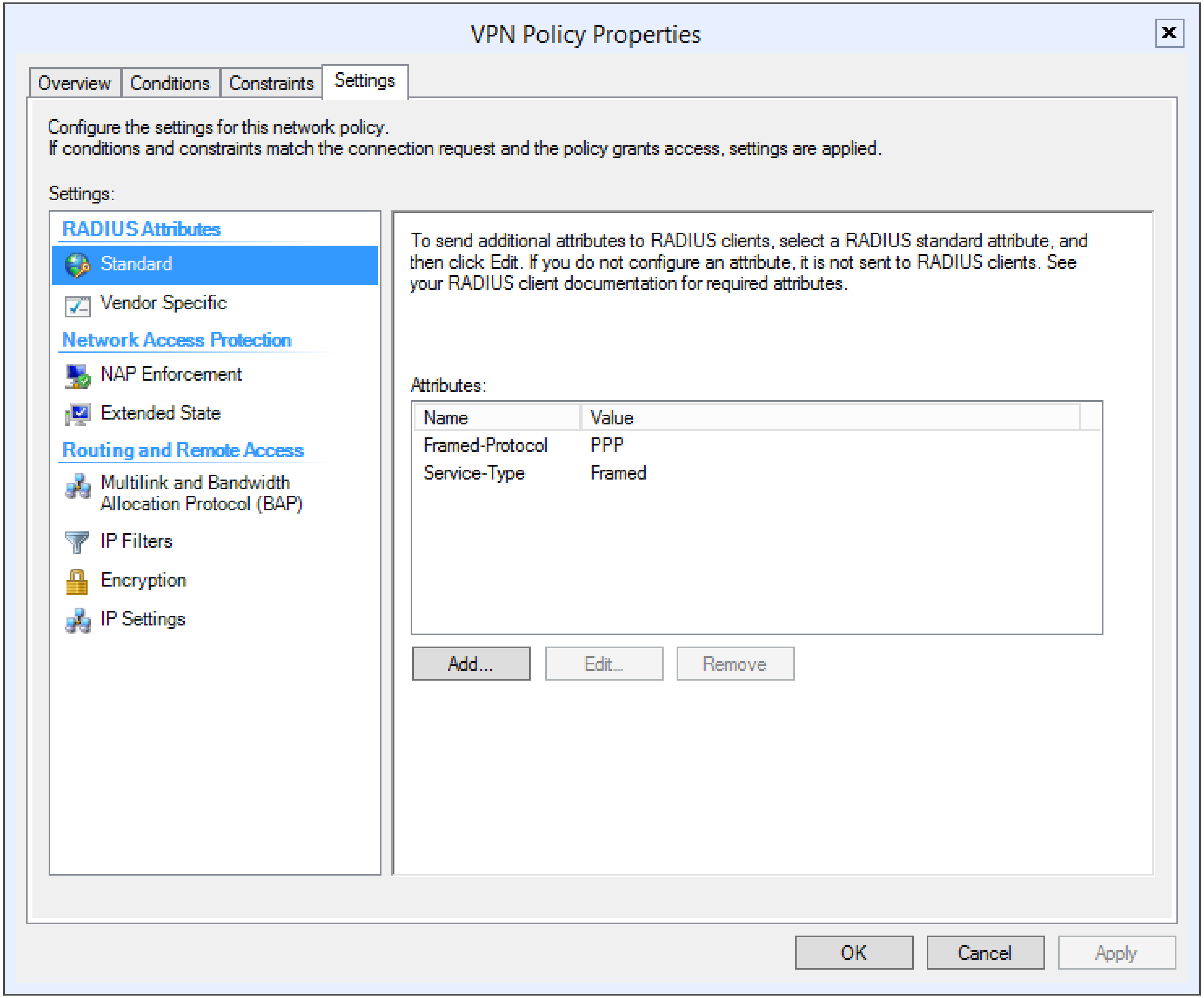
□ User can change password after it has expired

☑ Encrypted authentication (CHAP)

□ Unencrypted authentication (PAP, SPAP)

□ Allow clients to connect without negotiating an authentication method

□ Perform machine health check only



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed