Lesson 14: Configuring Network Access Protection (NAP)

MOAC 70-411: Administering Windows Server 2012

Microsoft Official Academic Course

WILEY

Overview

- Exam Objective 4.3: Configure Network Access Protection (NAP)
- Using Network Access Protection (NAP)

Using Network Access Protection (NAP)

Lesson 14: Configuring Network Access Protection (NAP)

Network Access Protection (NAP)

- NAP is Microsoft's software for controlling network access for computers based on the health of the host.
- NAP can be used on any computer that runs Windows and supports NAP.
- Types of computers that connect to a network:
  - Desktop computers
  - Roaming laptops
  - Unmanaged home computers
  - Visiting laptops

NAP Built-In Enforcement Methods

DHCP

IPsec

VPN

802.1*x*

Remote Desktop Gateway (RD Gateway)

NAP Architecture Components

- NAP client-side components
- NAP enforcement points
- NAP health policy server
- System Health Agents (SHAs)

NAP Architecture Components (cont.)

- Statement of Health (SoH)
- NAP Agent
- Health Registration Authority (HRA)
- Health requirements server
- Remediation servers

NAP Connection Process

1. When the NAP client connects to a network that requires NAP, each SHA on the NAP client validates its system health and generates an SoH.
2. The NAP client combines the SoHs from multiple SHAs into a SSoH and sends the information to a NAP health policy server that is defined with the NAP enforcement point.
3. The NAP health policy server uses its installed SHVs and the health requirements policies to determine whether the NAP client meets health requirements.

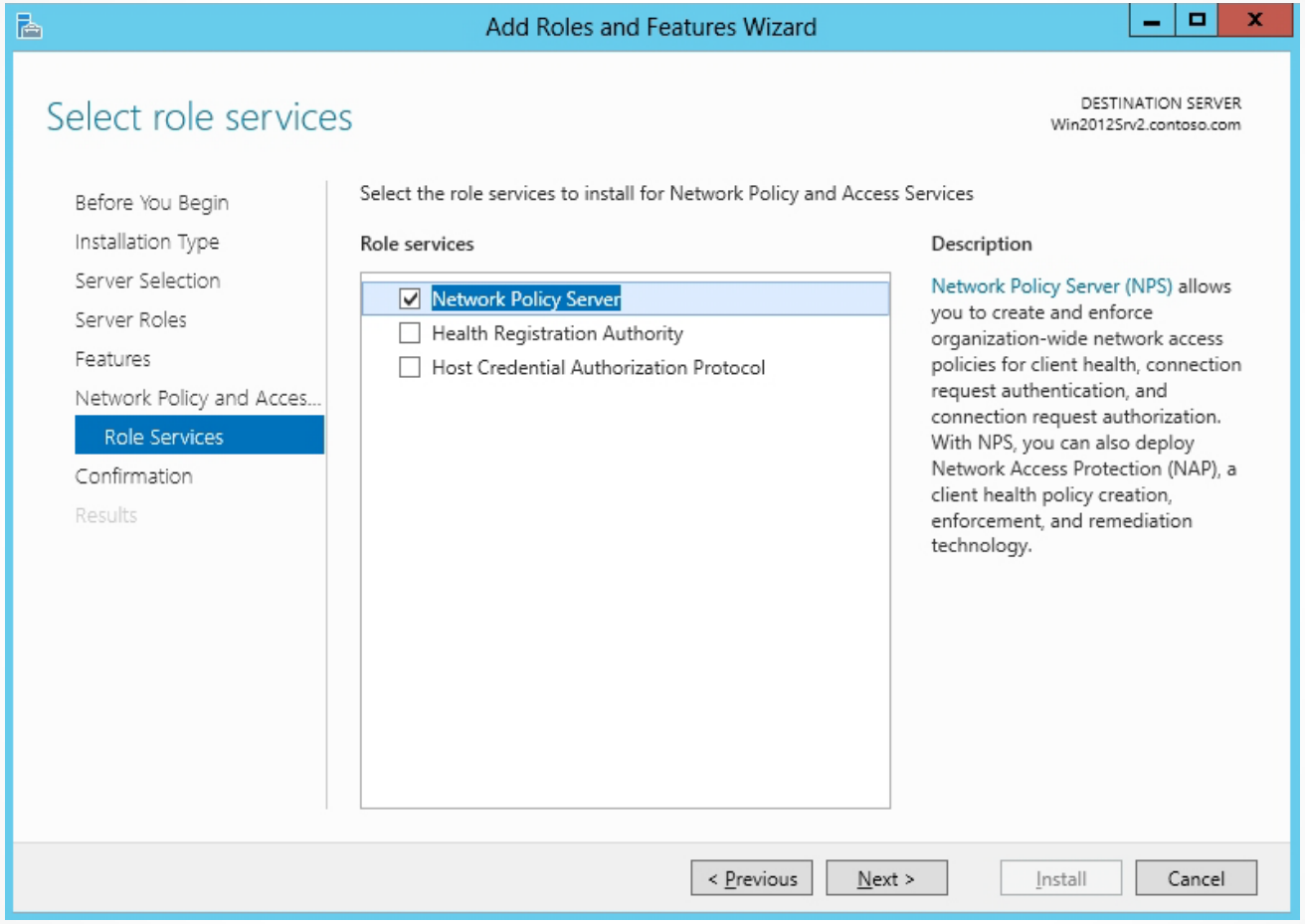
NAP Connection Process

4. The NAP health policy server combines the SoHRs from the multiple SHVs into a System Statement of Health Response (SSoHR) and sends the SSoHR back to the NAP client through the NAP enforcement point.
5. If the client is compliant, the enforcement point allows the connection. If the client is noncompliant, the computer can be connected to a remediation network.
6. If the computer is noncompliant, the noncompliant computer can attempt to come into compliance.
7. If the status of the computer changes, the entire process starts over.

Installing Network Access Protection

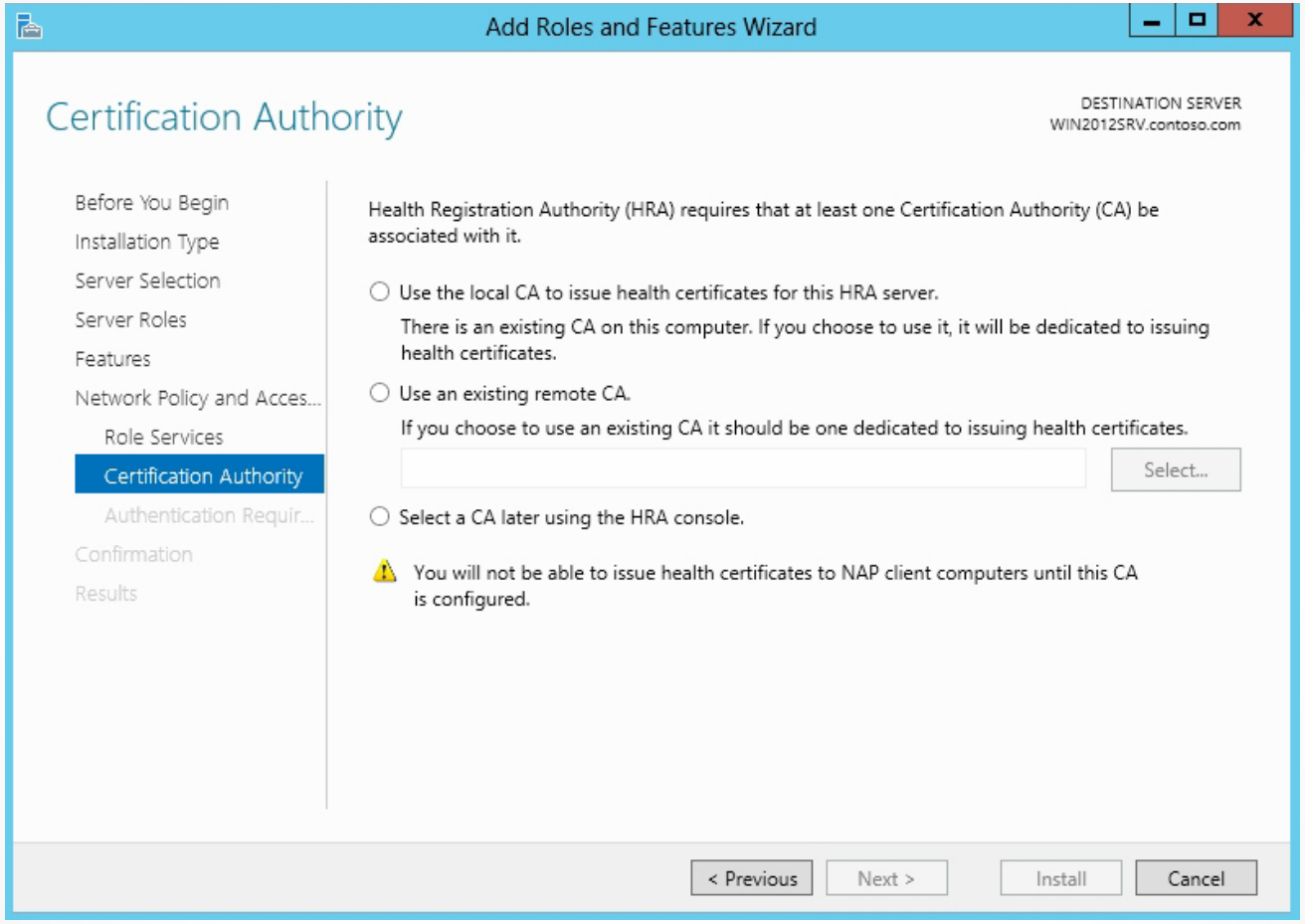
- Because NAP is offered through NPS, the installation is similar to installing NPS (discussed in Lesson 12).
- However, you want to add HRA, which is used to issue health certificates to NAP client computers that are compliant with network health requirements.
- For HRA to function, you need to have a CA available.

Install Network Policy Server



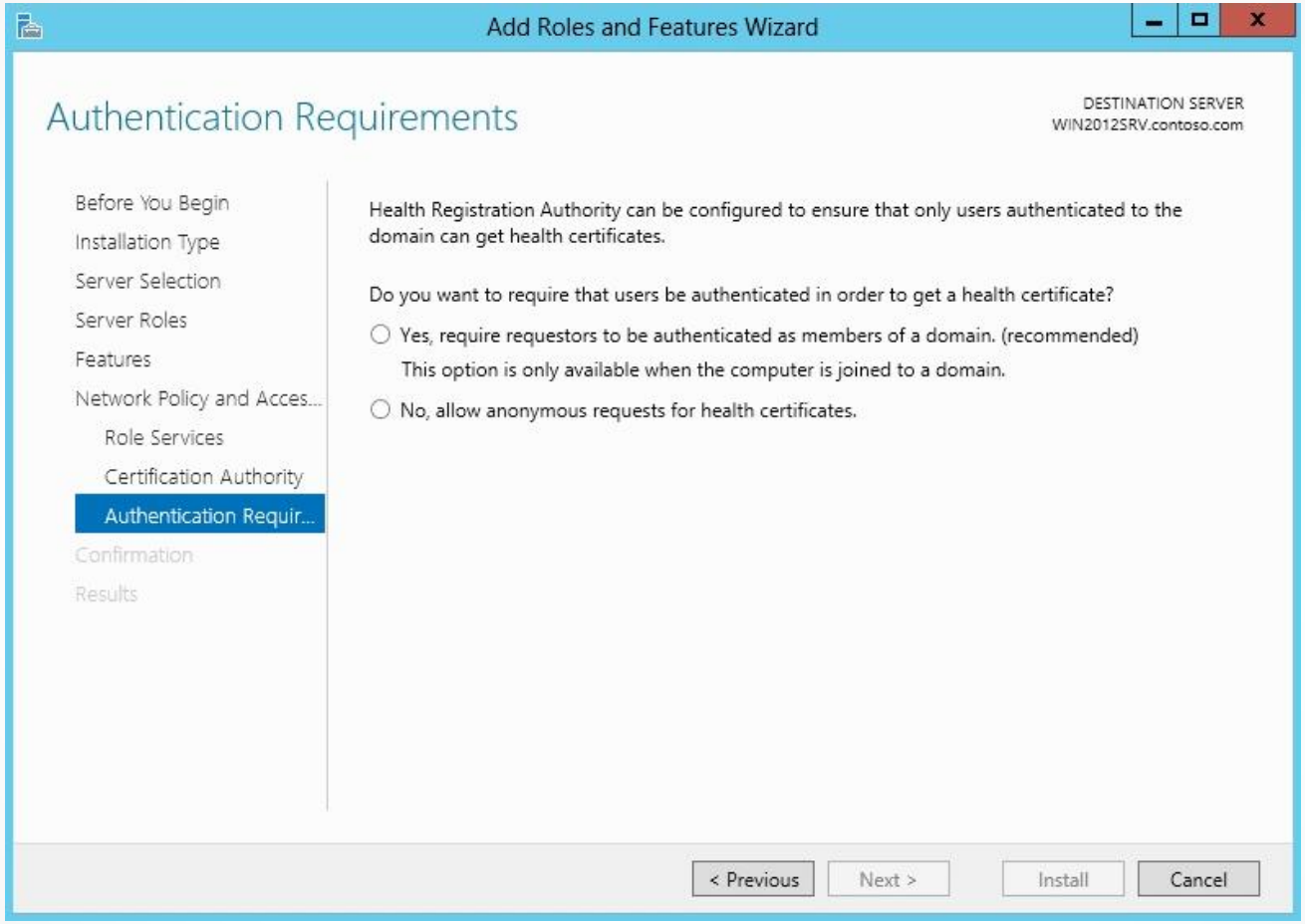
Selecting the role services

Install Network Policy Server



Specifying the Certificate Authority

Install Network Policy Server



Configuring the authentication requirements

Configuring NAP Enforcement

To configure NAP:

1. Install and configure the server on which you will apply NAP enforcement.
2. Configure NPS and the NAP-related policies.
3. Configure the remediation servers.

DHCP Enforcement

To control network access, DHCP enforcement sets the following:

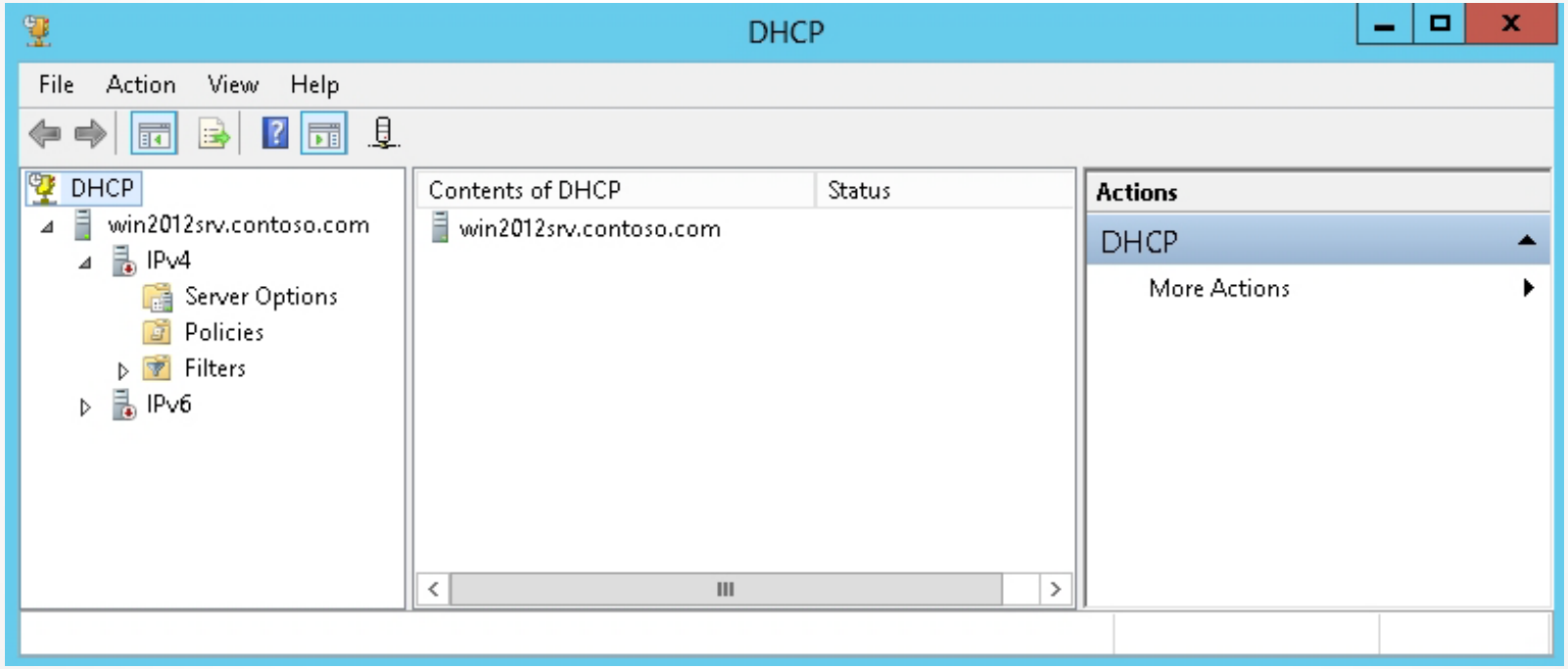
- DHCP Router option is set to 0.0.0.0 so noncompliant computers do not have a configured default gateway.
- Subnet mask is set to 255.255.255.255 so that there are no routes to the attached subnet.

Configuring NAP Enforcement for DHCP

To configure DHCP enforcement, you must:

1. Configure a DHCP server and create the appropriate DHCP scopes.
2. Install NPS on the DHCP server.
3. Run the NAP Wizard to configure the connection request policy, network policy, and NAP health policy. Define the remediation severs, which noncompliant clients can access.
4. Enable NAP for individual DHCP scopes.
5. Enable the NAP DHCP Quarantine Enforcement Client and start the NAP service on NAP-capable client computers.

Configure the DHCP Server

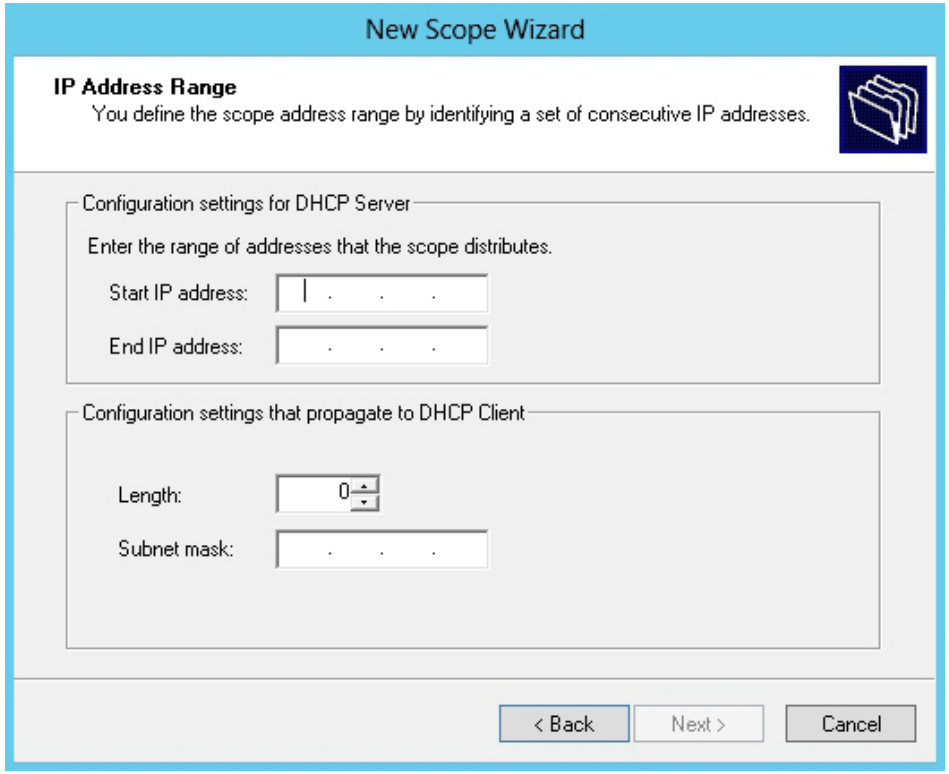


Opening the DHCP console

Configure the DHCP Server

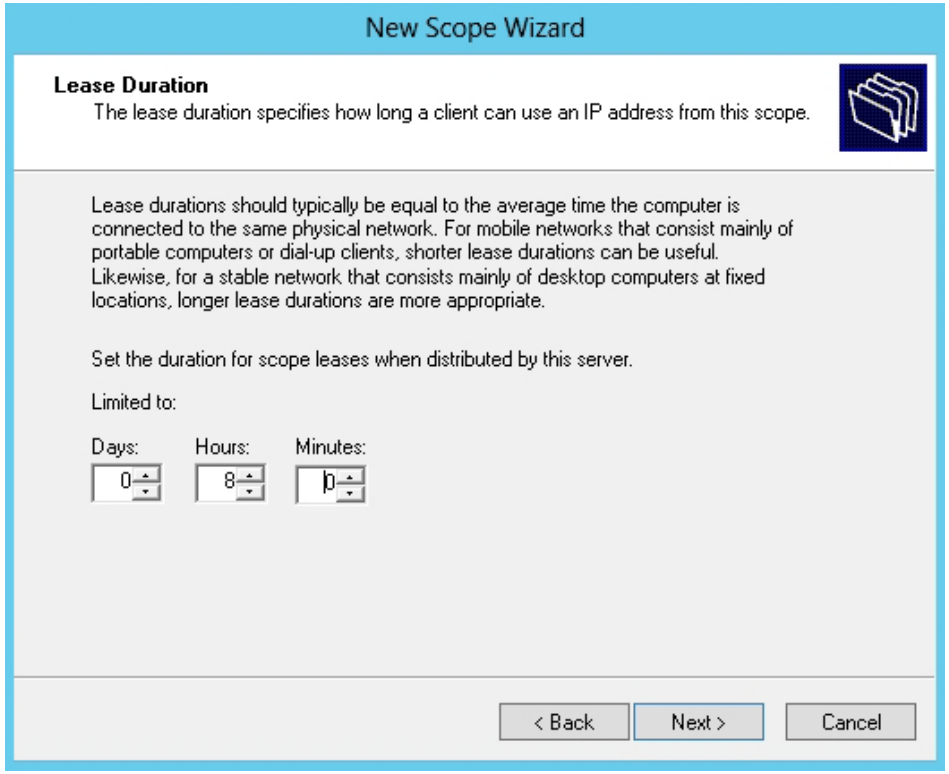
Defining the scope name

Configure the DHCP Server



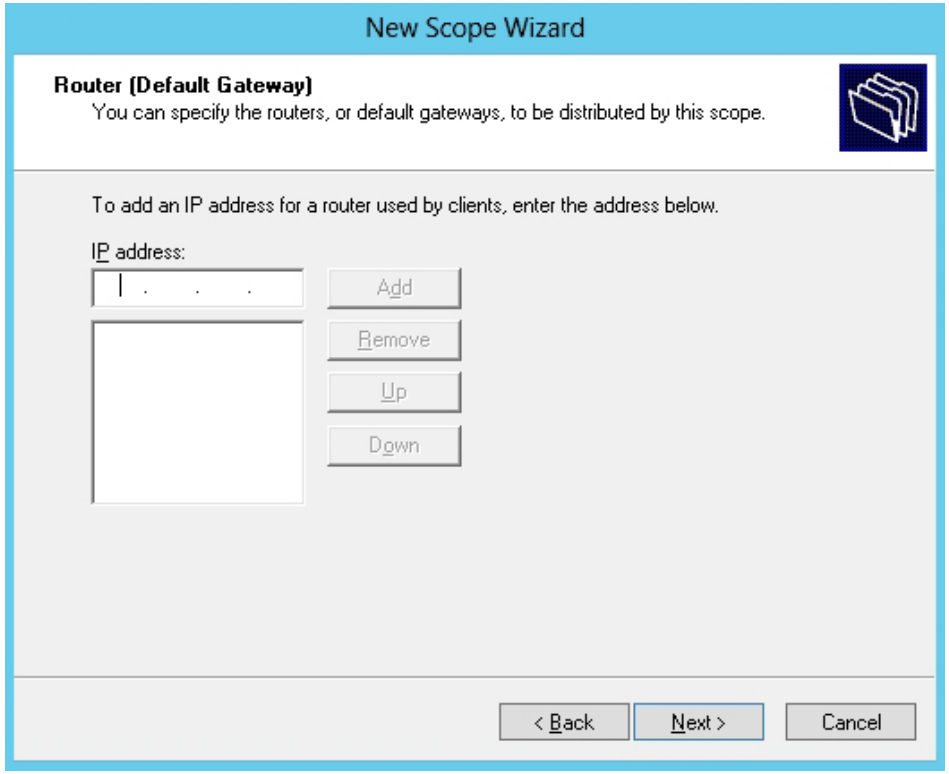
Specifying the IP address range

Configure the DHCP Server



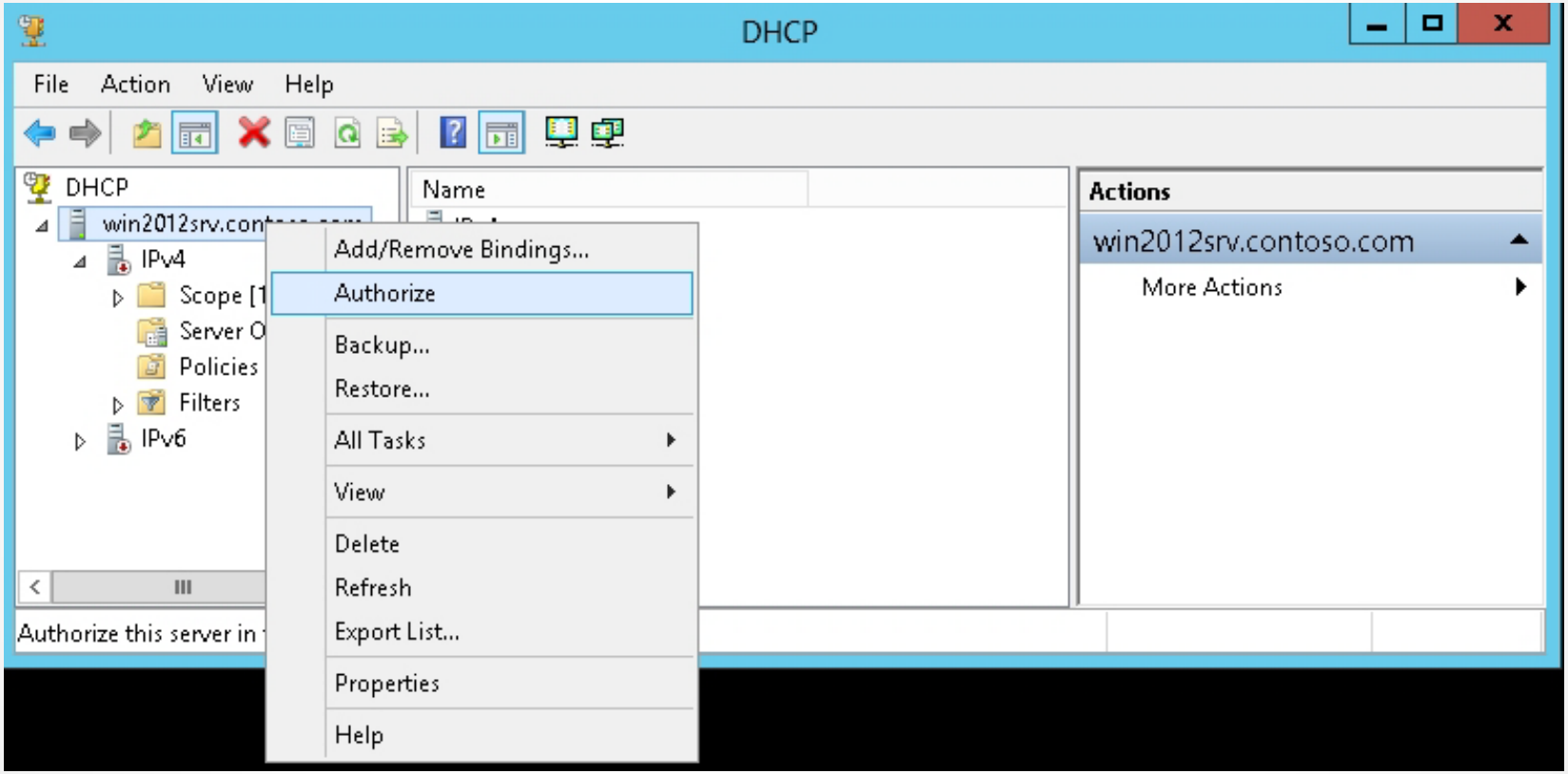
Specifying the lease duration

Configure the DHCP Server



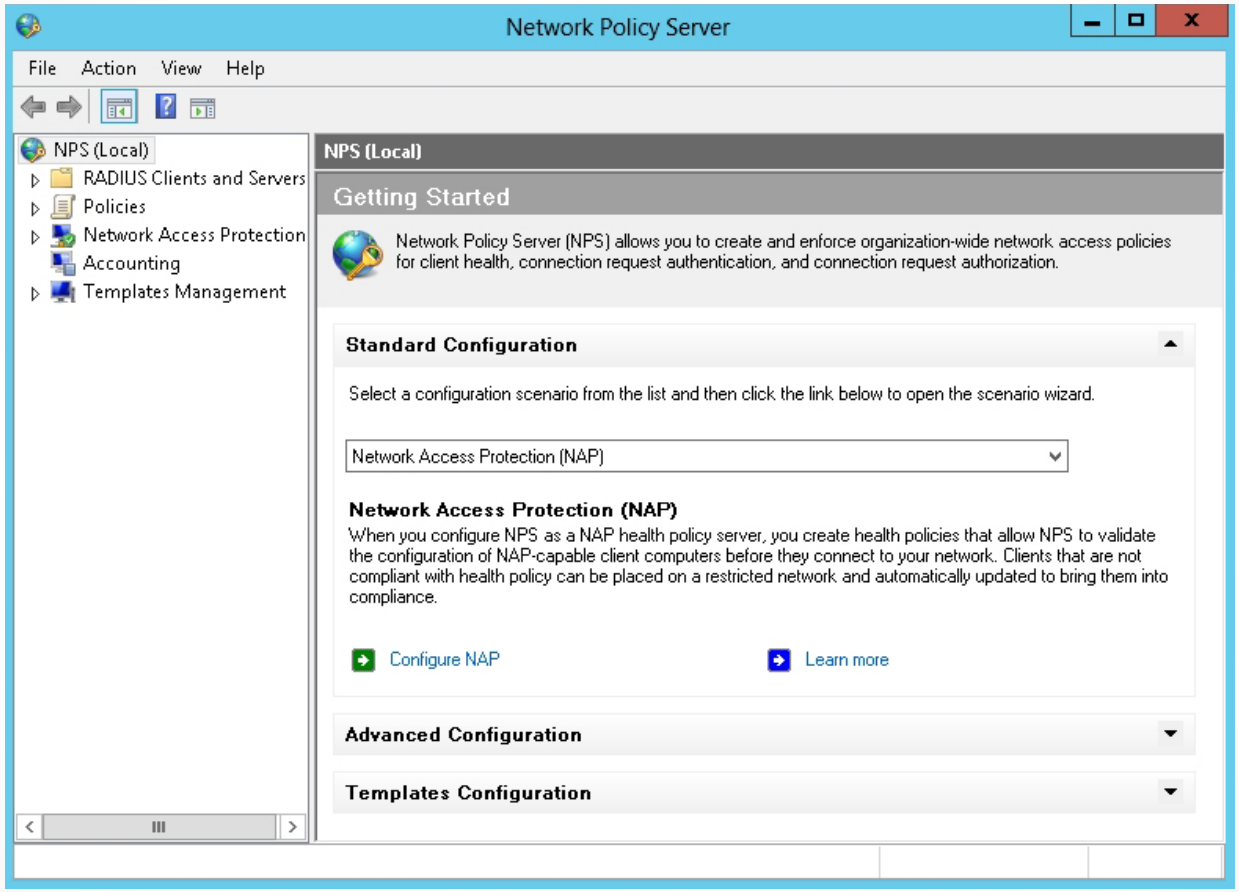
Defining the default gateway

Configure the DHCP Server



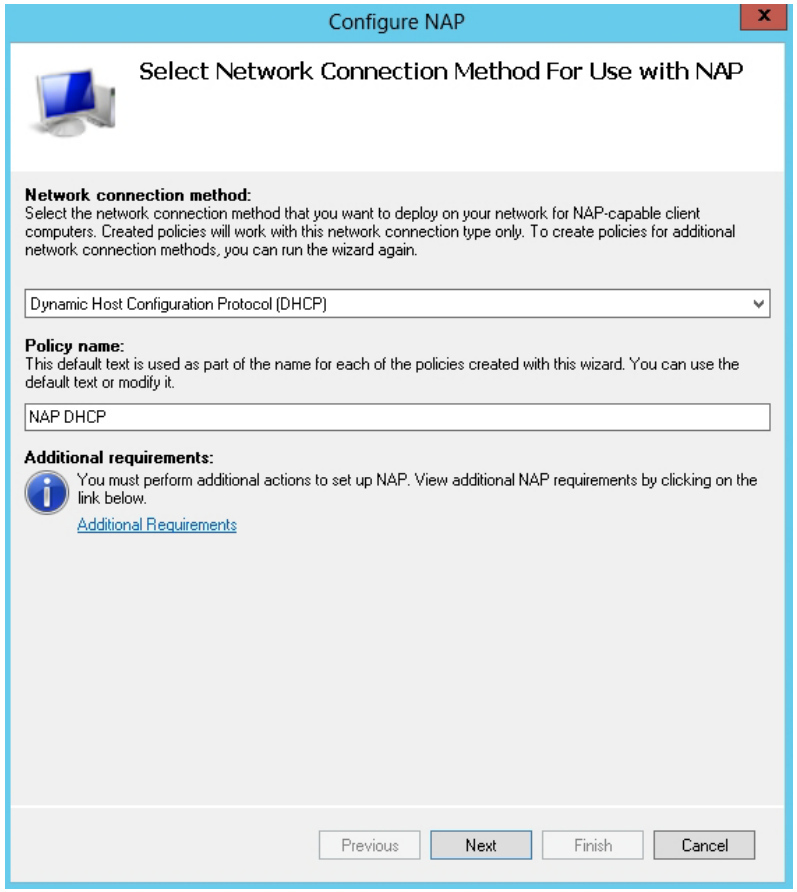
Authorizing the DHCP server

Configure NAP for DHCP Server



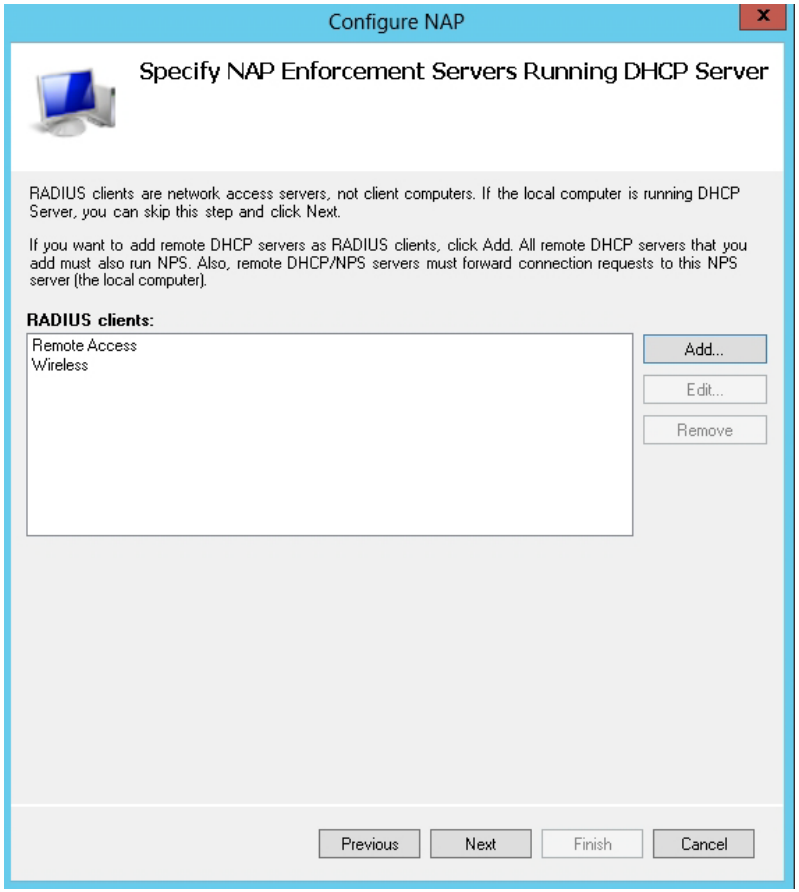
Starting the Network Policy Server console

Configure NAP for DHCP Server



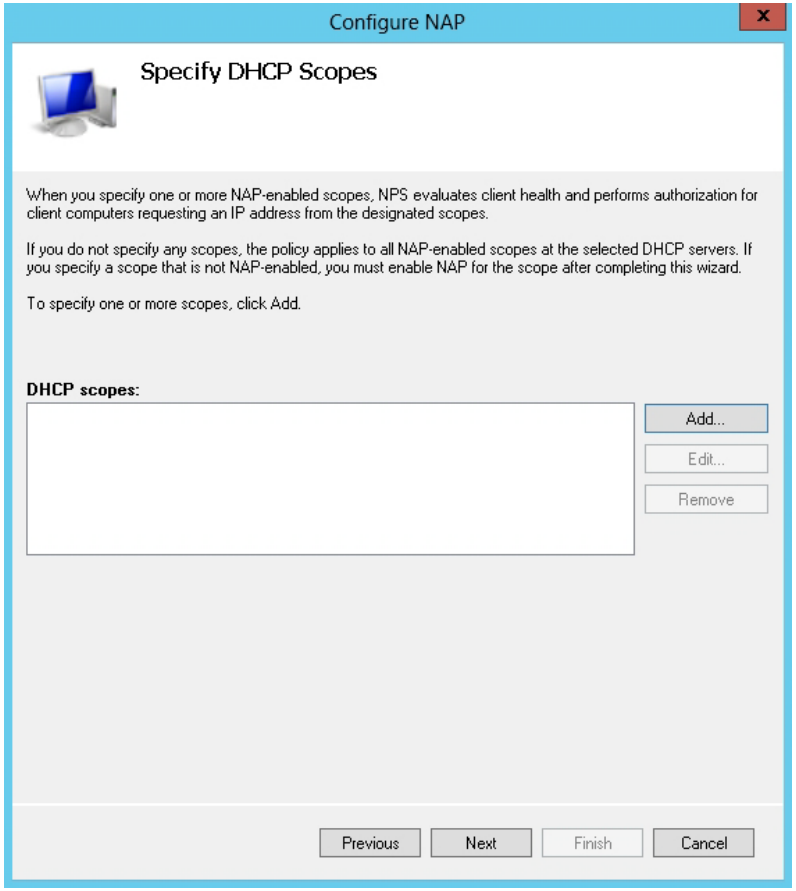
Selecting the network connection method

Configure NAP for DHCP Server



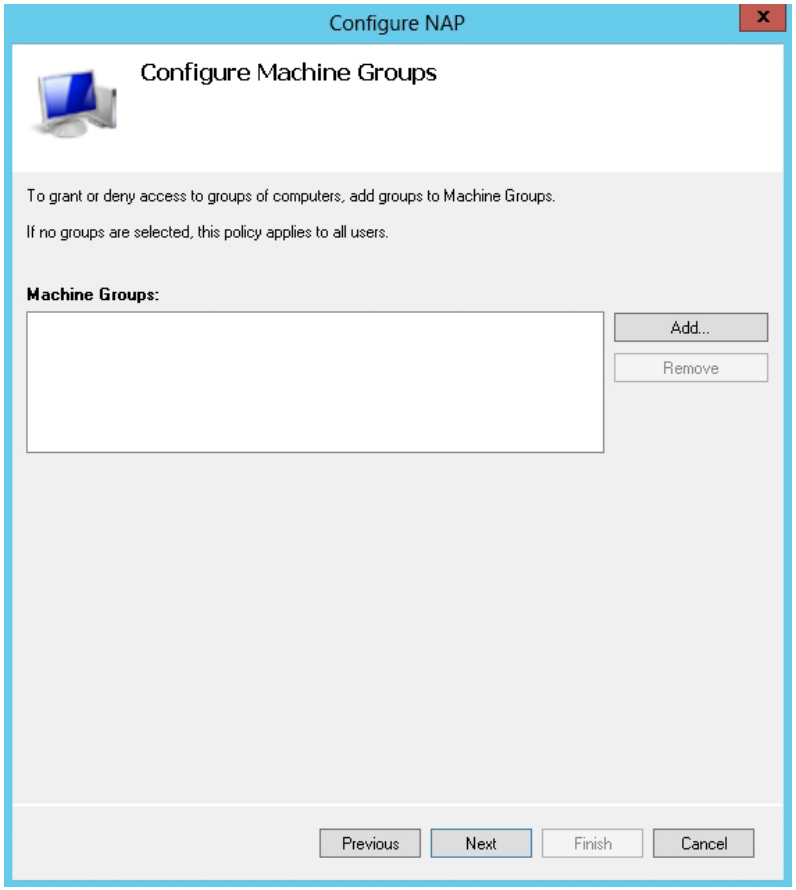
Specifying NAP enforcement servers running DHCP server

Configure NAP for DHCP Server



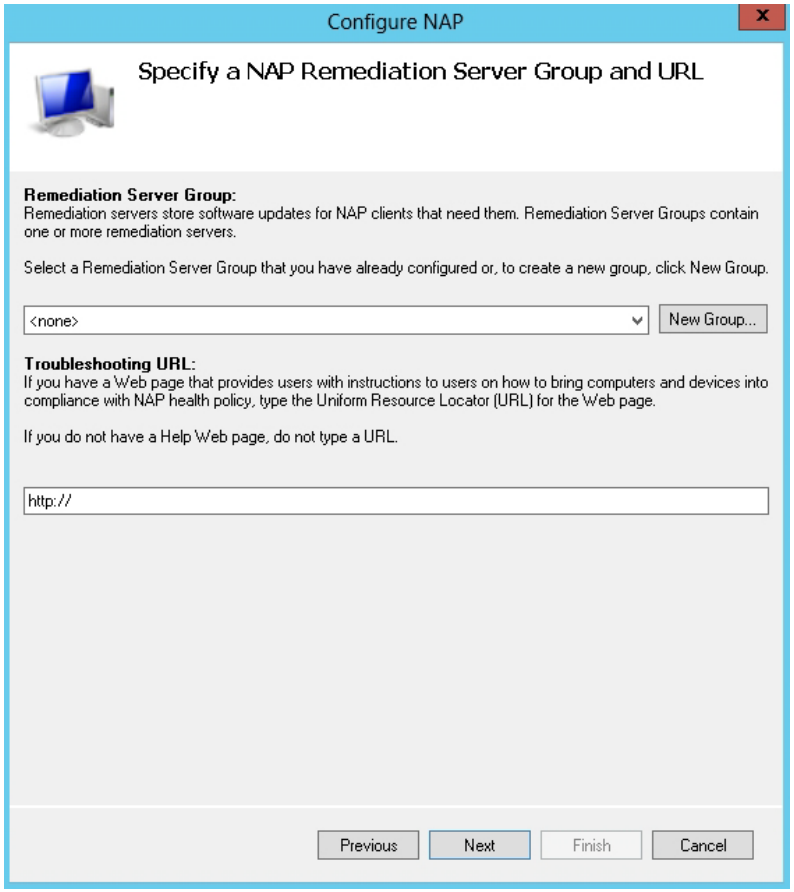
Specifying the DHCP scopes to apply to NAP

Configure NAP for DHCP Server



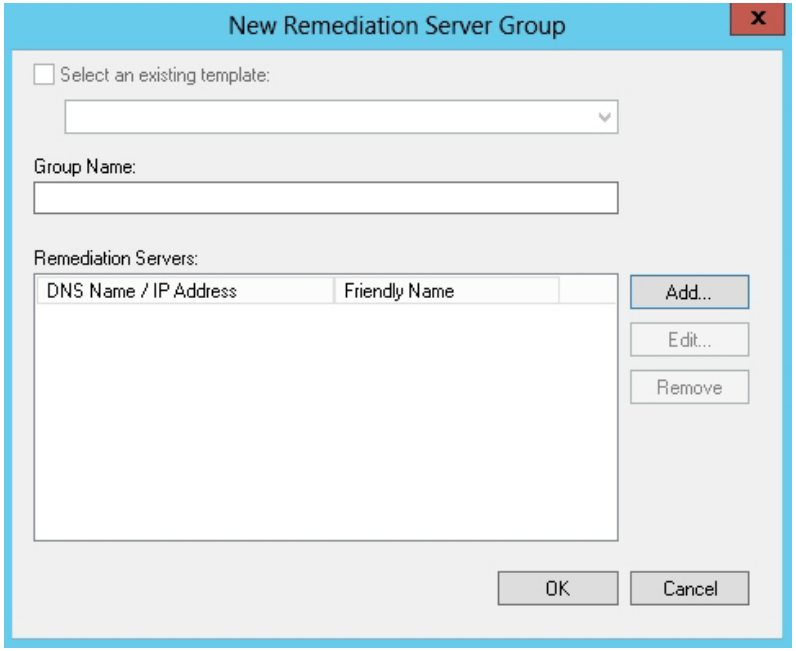
Specifying the computer groups that NAP will apply to

Configure NAP for DHCP Server



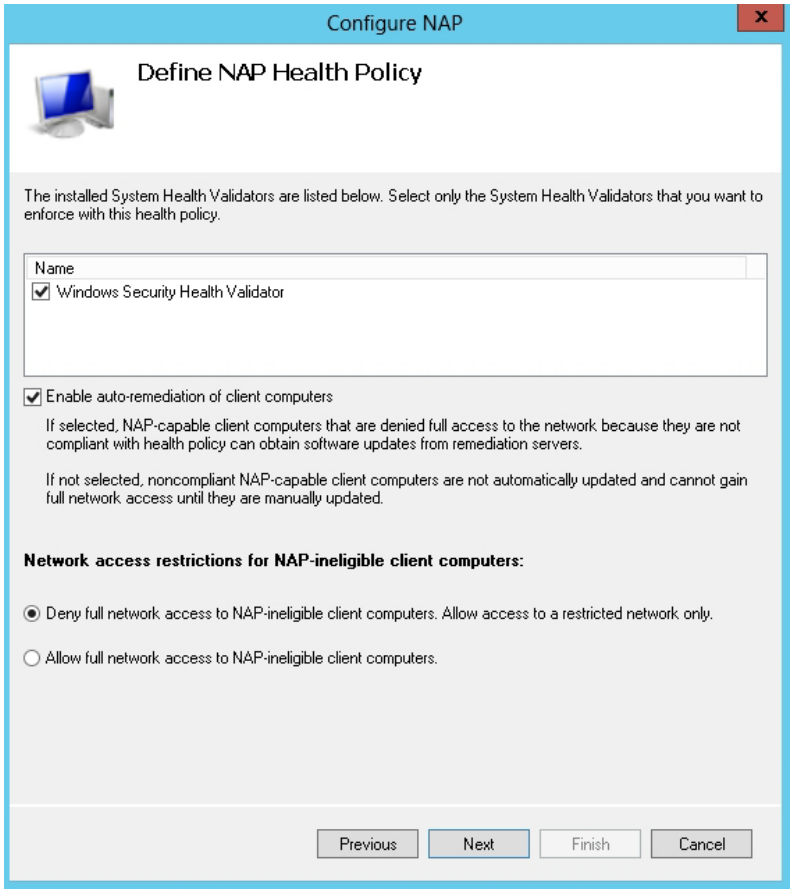
Specifying the NAP Remediation Server group and URL

Configure NAP for DHCP Server



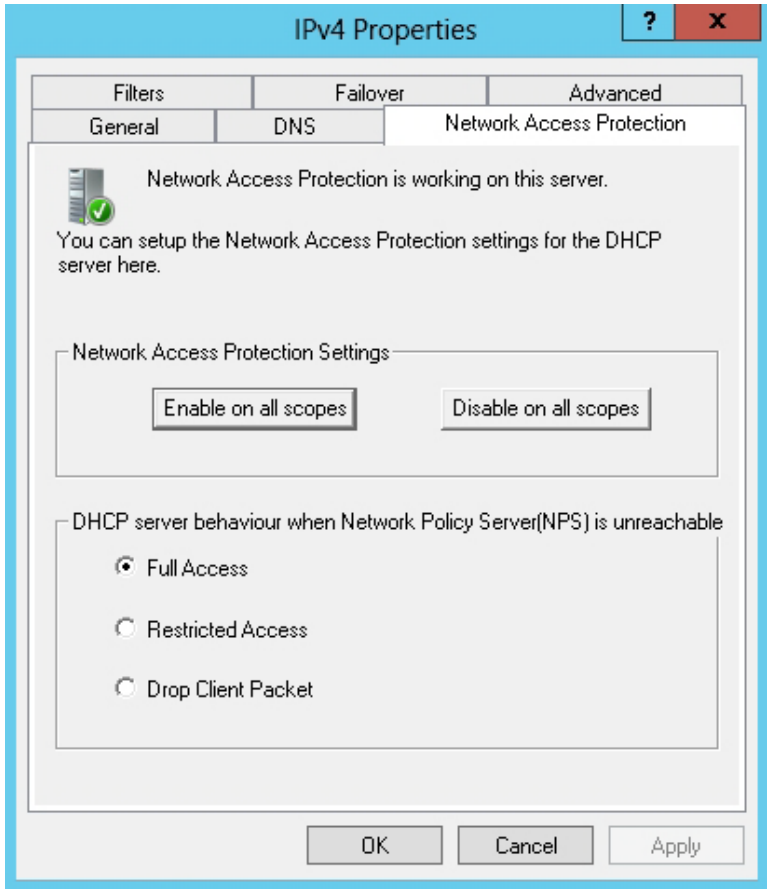
Adding computers to the Remediation Server group

Configure NAP for DHCP Server



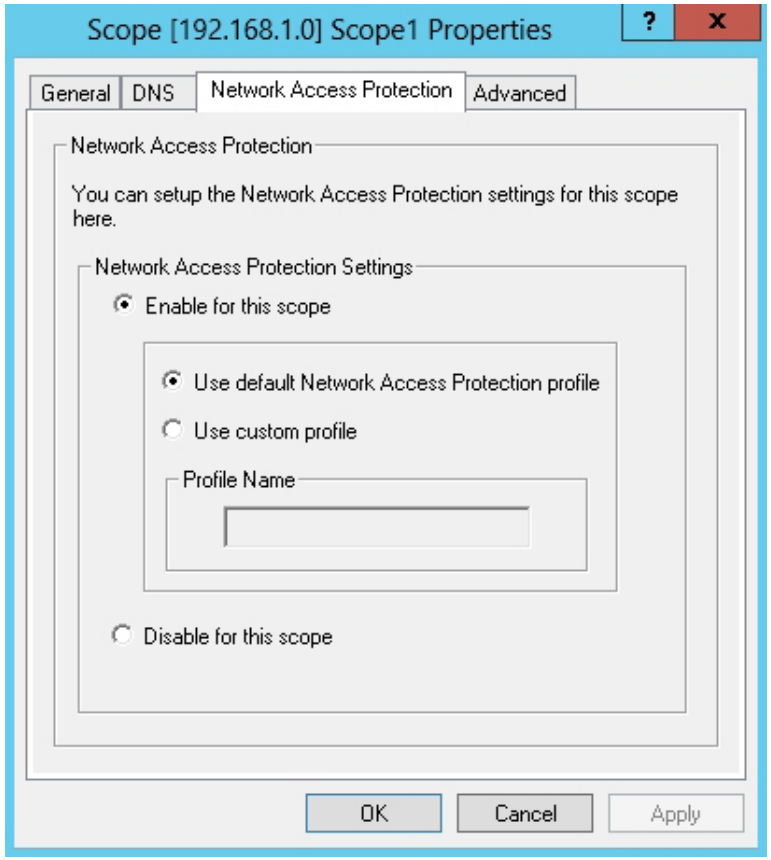
Defining NAP Health Policy

Enable NAP on All DHCP Scopes



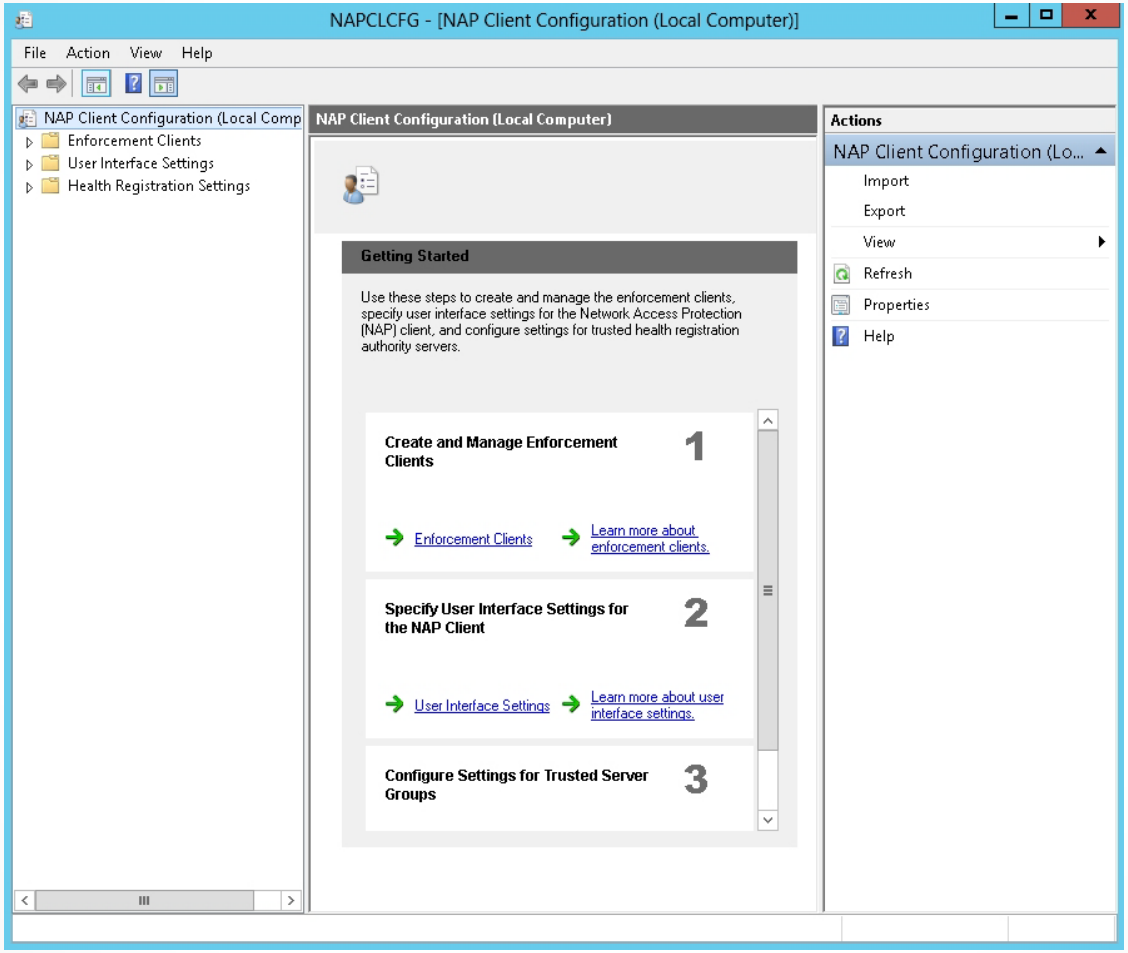
Enabling NAP for all DHCP scopes

Enable NAP on an Individual DHCP Scope



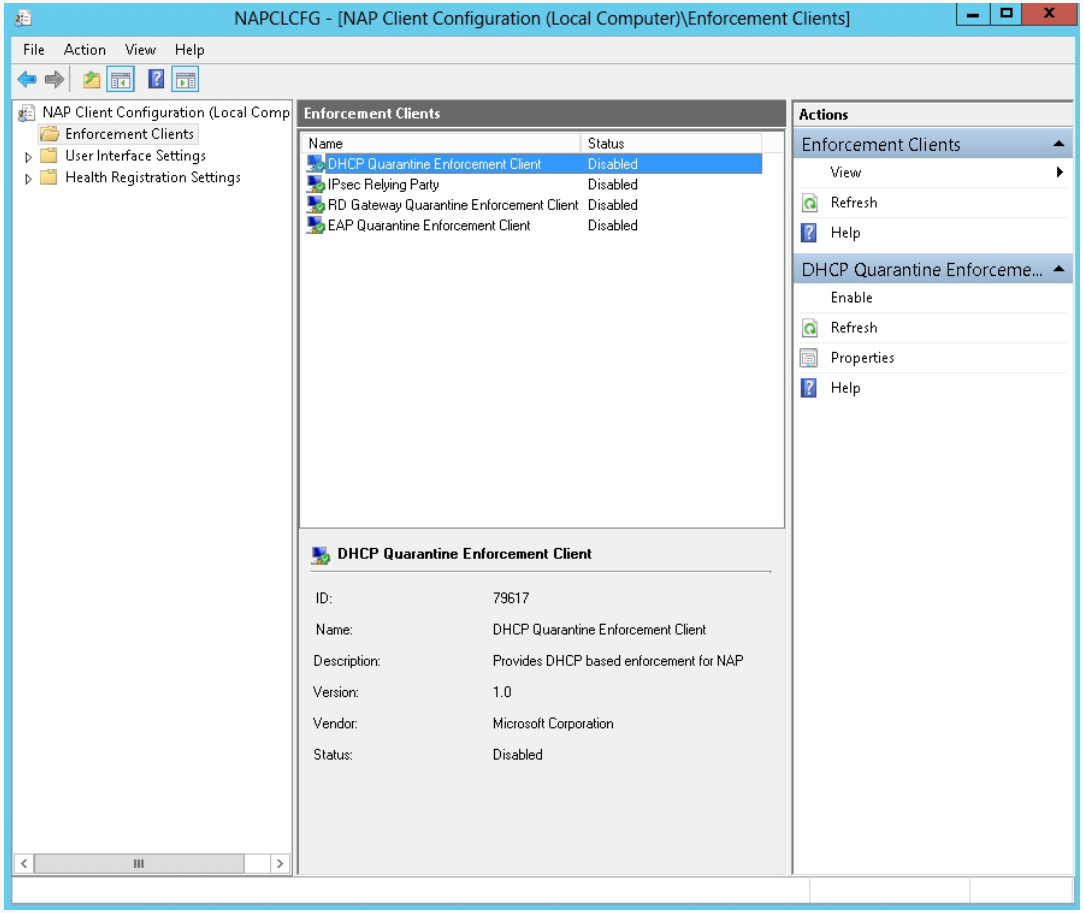
Enabling NAP for individual DHCP scopes

Enable the NAP DHCP Quarantine Enforcement Client and Start NAP Service on a DHCP Server



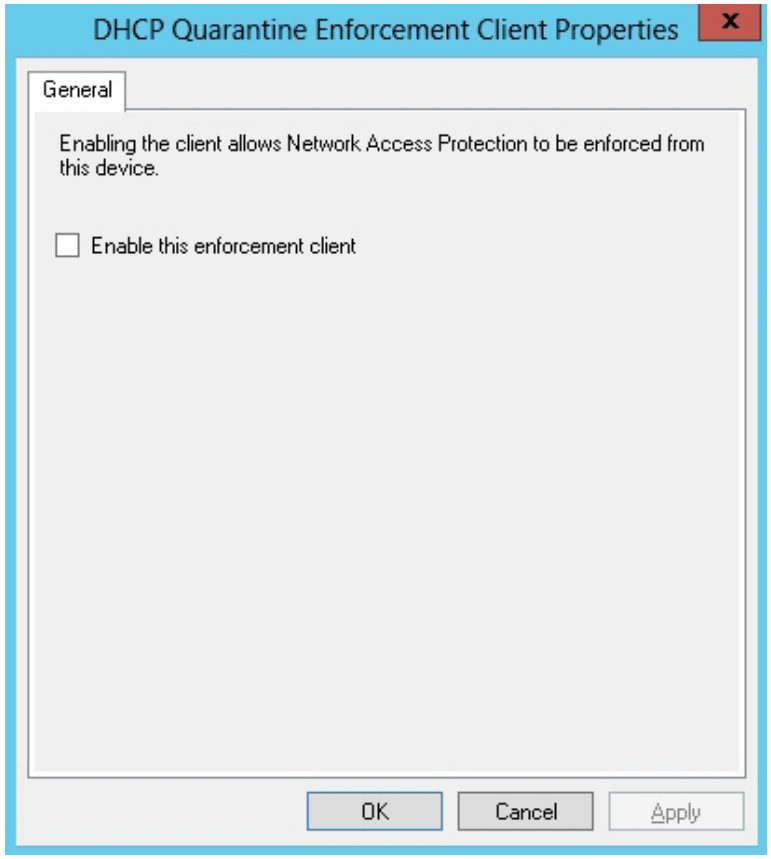
Opening the NAP Client Configuration console

Enable the NAP DHCP Quarantine Enforcement Client and Start NAP Service on a DHCP Server



Configuring the enforcement clients

Enable the NAP DHCP Quarantine Enforcement Client and Start NAP Service on a DHCP Server

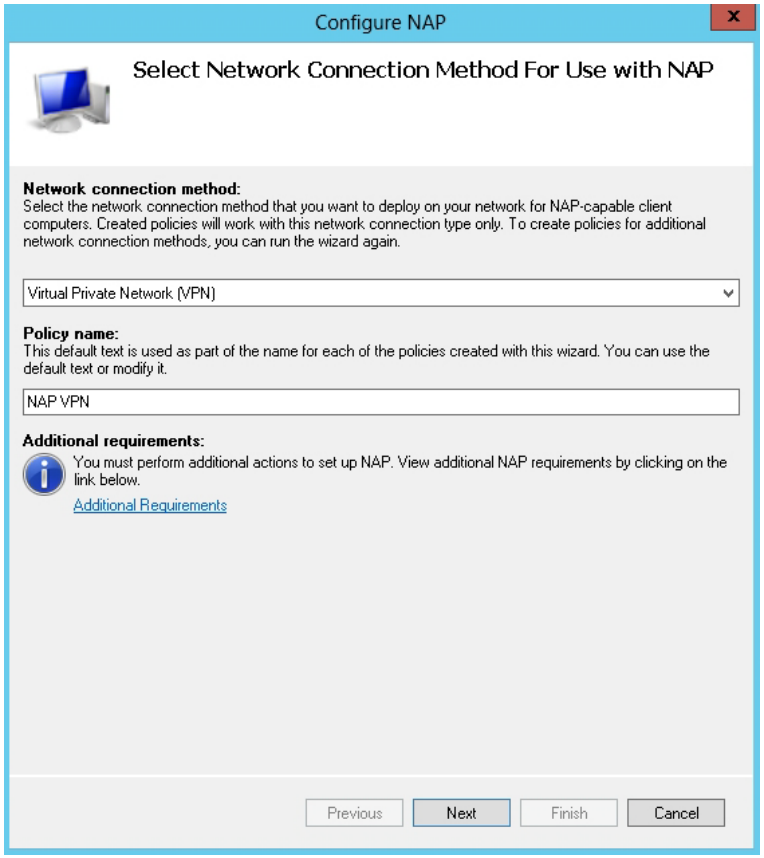


Enabling enforcement client for DHCP

Configuring NAP Enforcement for VPN

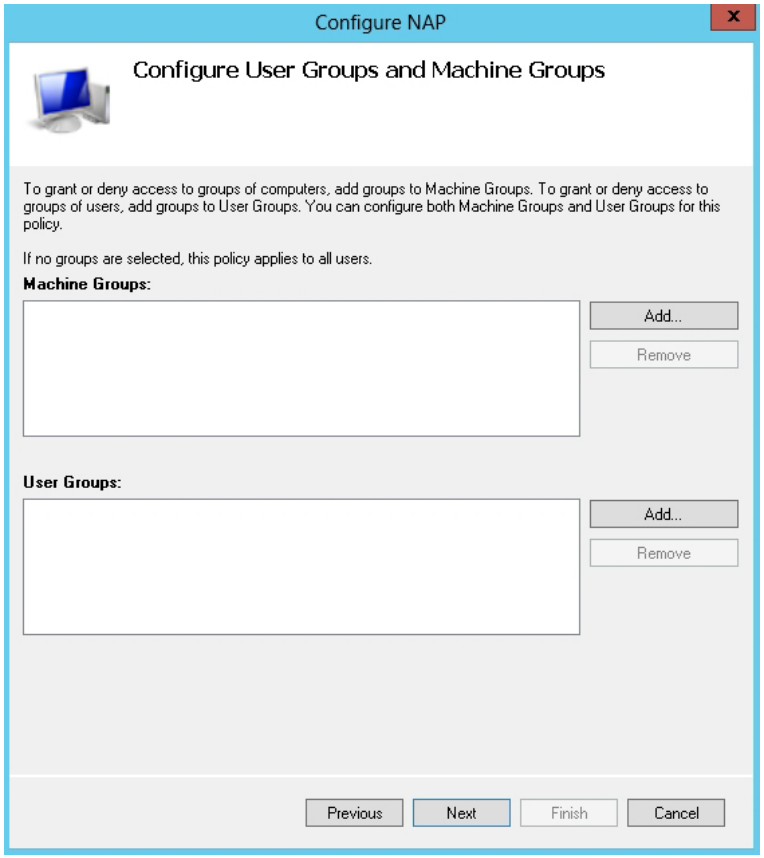
1. Install NPS on the VPN server.
2. Configure the VPN server and have them use PEAP-based authentication (either PEAP-MS-CHAP v2 or PEAP-TLS).
3. Run the NAP Wizard to configure the connection request policy, network policy, and NAP health policy. Define the remediation severs, which noncompliant clients can access.
4. Enable the NAP DHCP Quarantine Enforcement Client and start the NAP service on NAP-capable client computers.

Configure NAP for VPN Servers



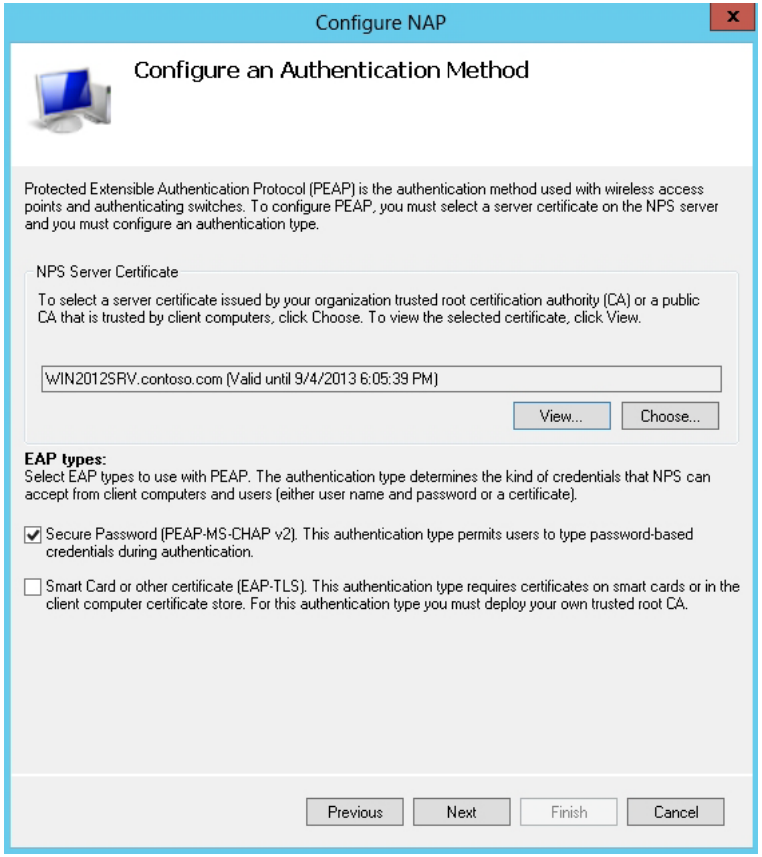
Selecting the Virtual Private Network (VPN) for the Network Connection

Configure NAP for VPN Servers



Specifying user and machine groups for NAP

Configure NAP for VPN Servers

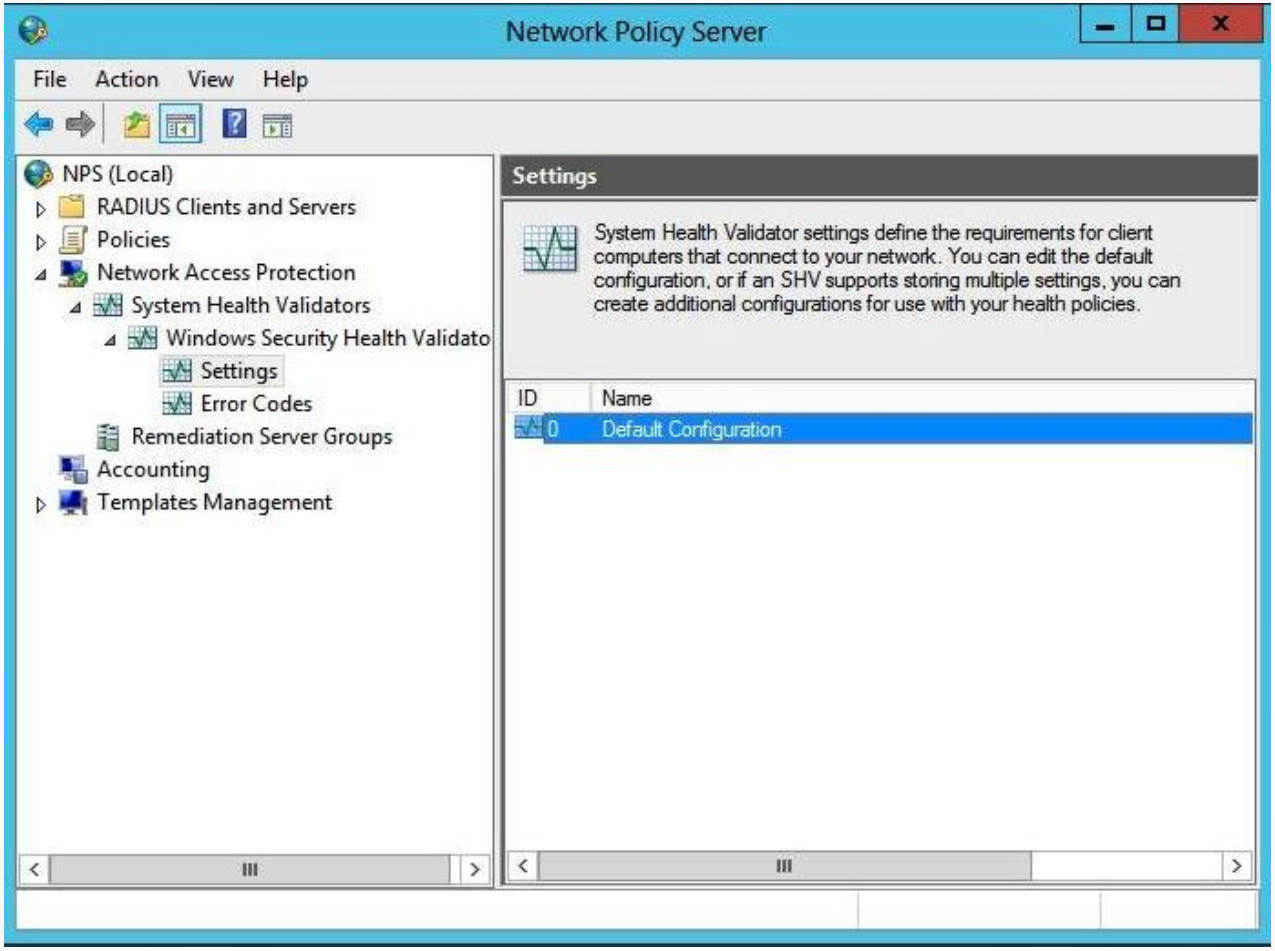


Configuring an authentication method for NAP

System Health Validators

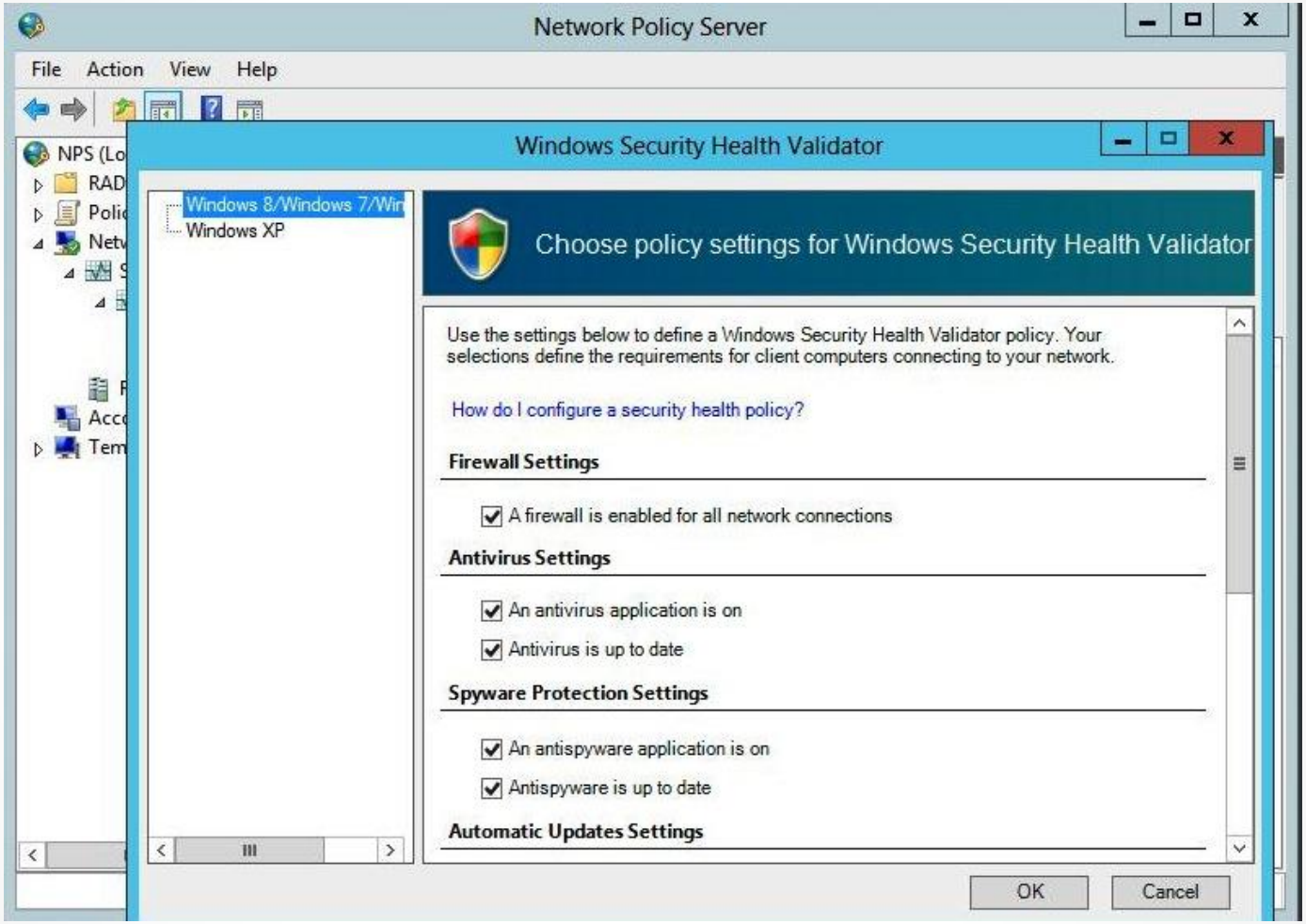
- ***System Health Validators (SHVs)*** settings define the requirements for client computers that connect to your network.
- You configure SHVs using the Network Policy Server console.
- Windows 8 includes a Windows Security Health Validator SHA that monitors the Windows Security Center settings.
- Windows Server 2012 includes a corresponding Windows Security Health Validator SHV.

System Health Validators



Managing the Windows SHV

System Health Validators



Configuring Windows SHV

Configuring System Health Validators

SHV options:

- Firewall Settings
- Antivirus Settings
- Spyware Protection Settings
- Automatic Updates Settings
- Security Updates Settings

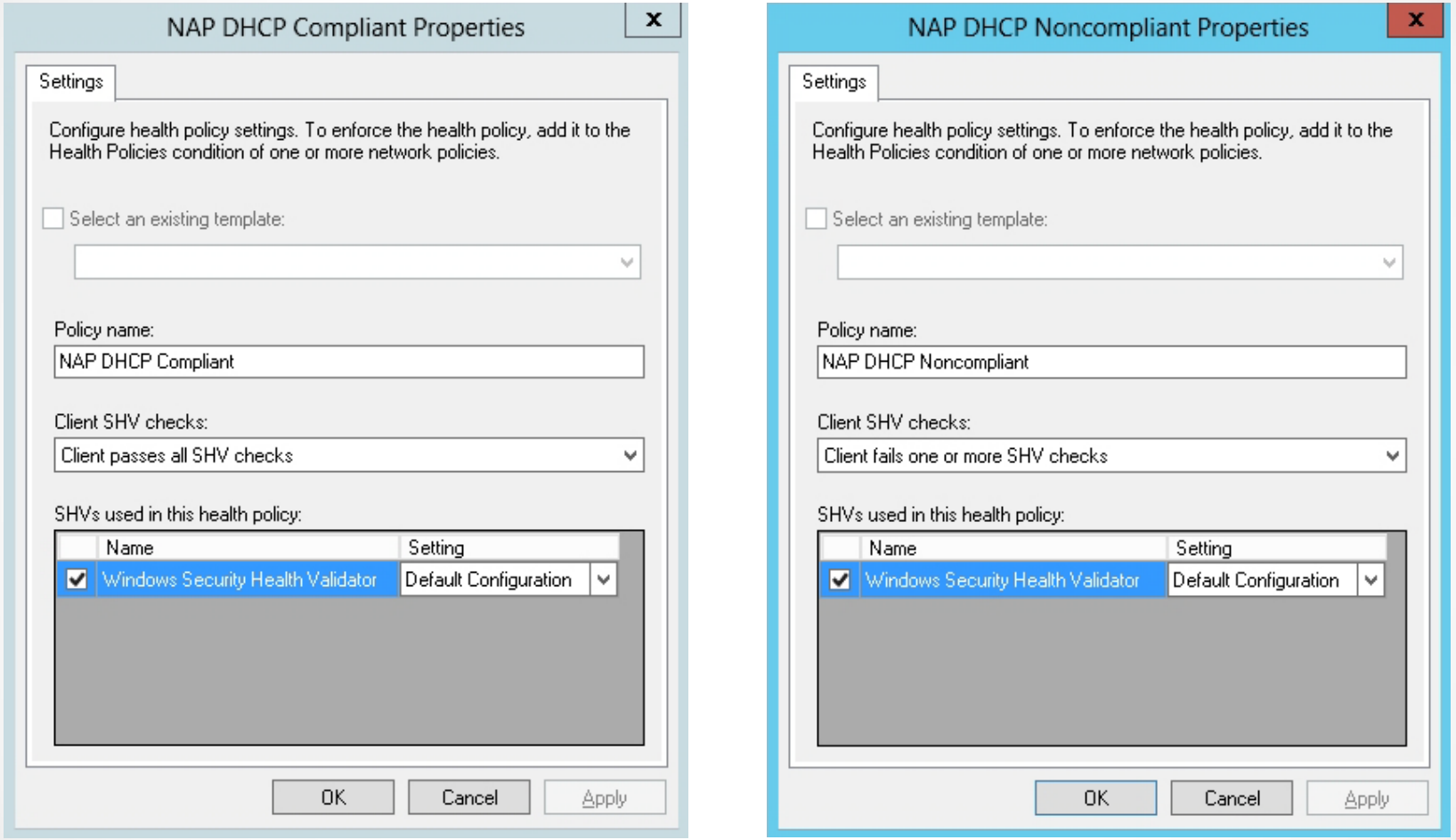
System Health Validators

Configuring Security Updates settings

Configuring Health Policies

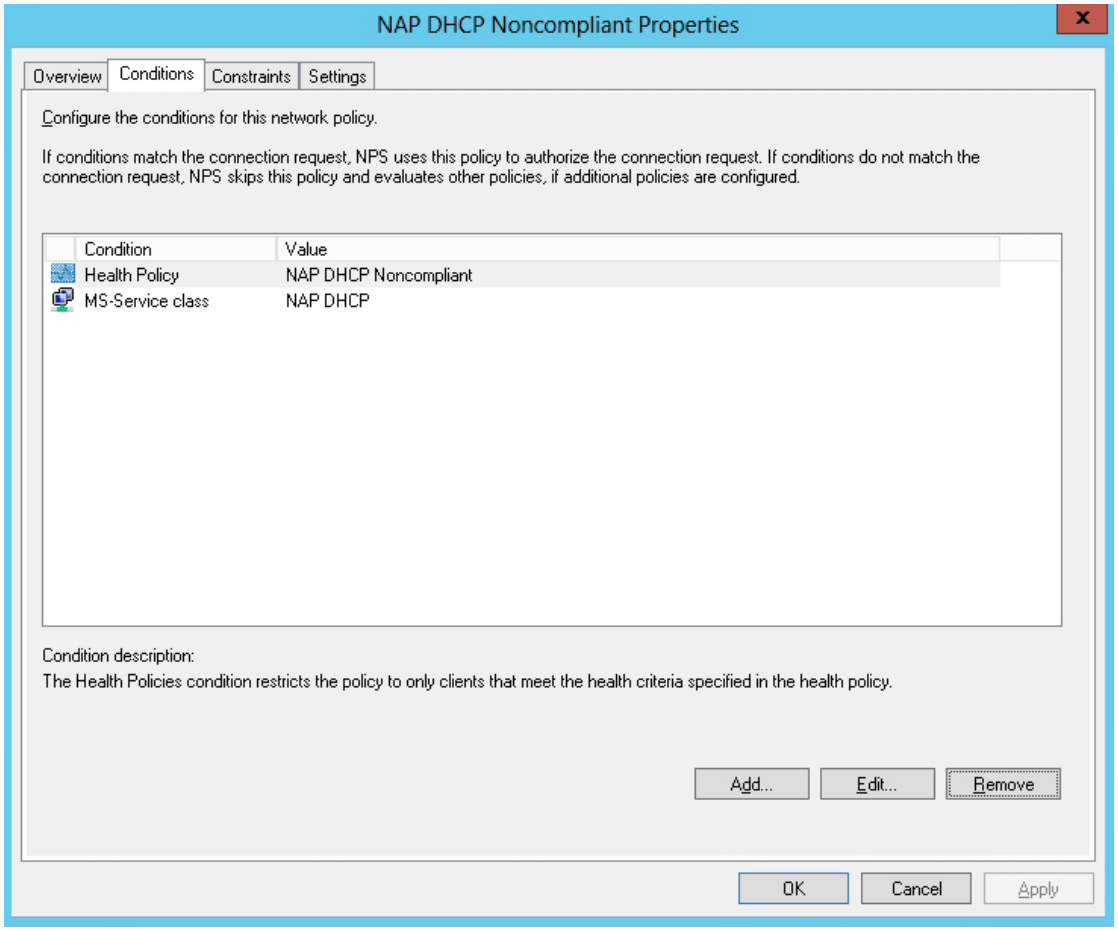
- Health policies consist of one or more system health validators and other settings that enable you to define client computer configuration requirements for the NAP-capable computers that attempt to connect to your network.
- Health policy pairs:
  - NAP-compliant
  - NAP-noncompliant

Configuring Health Policies



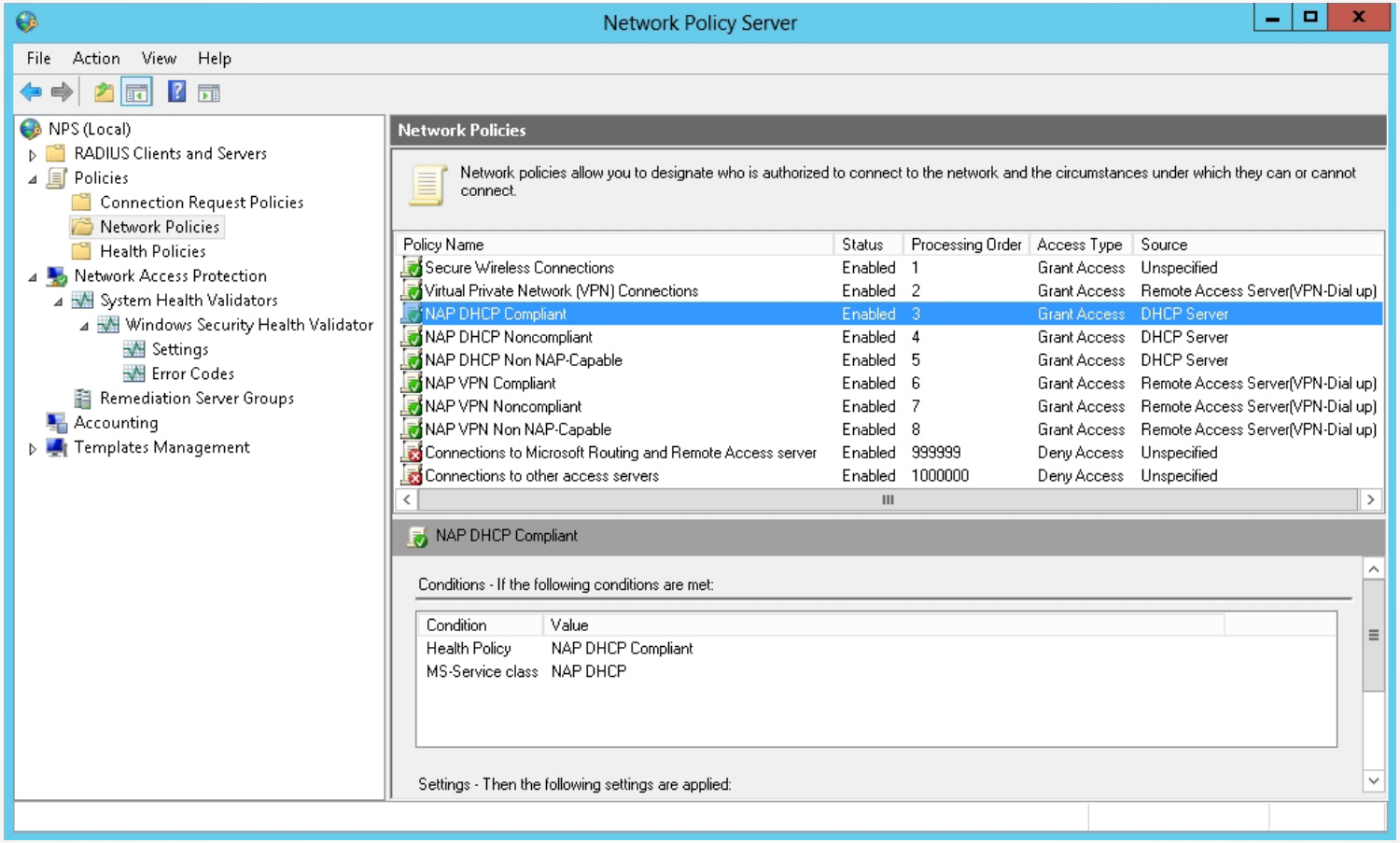
Viewing the health policies

Configuring Health Policies



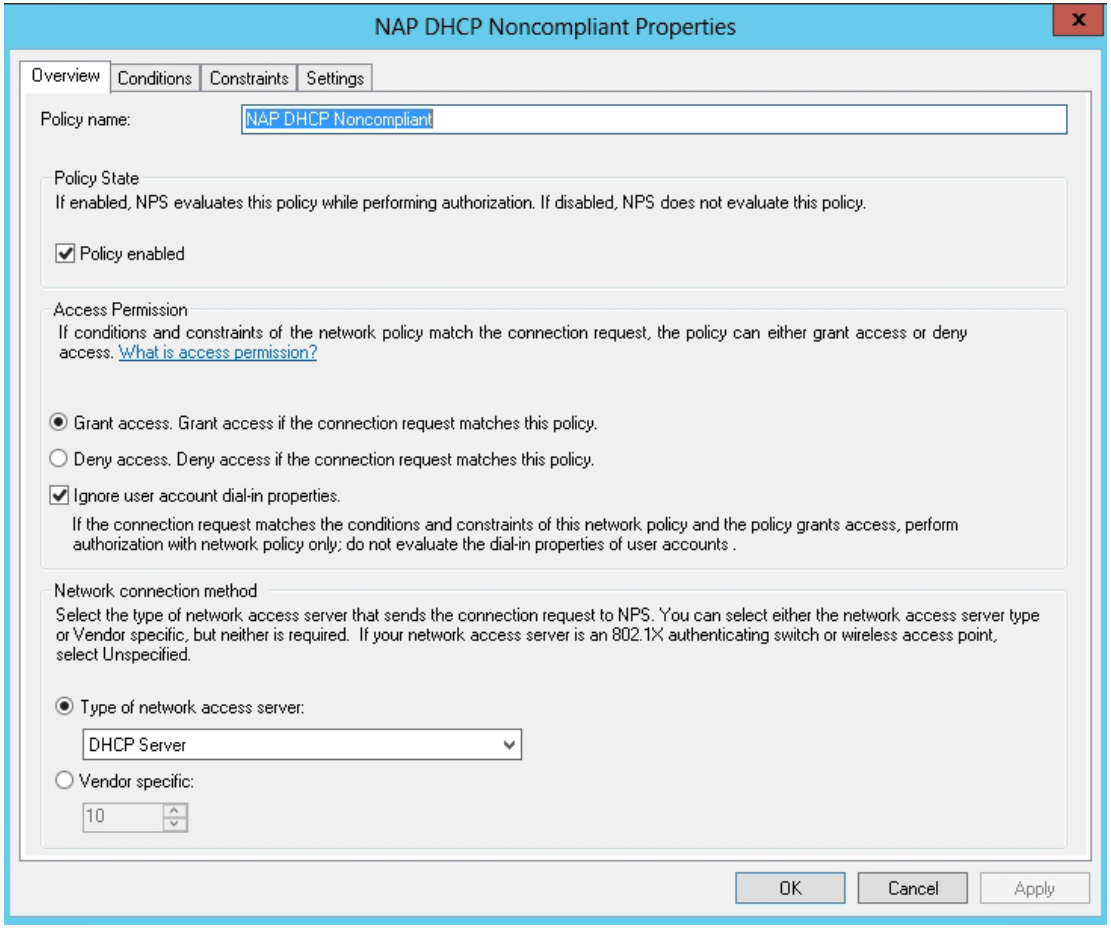
Displaying the conditions of a health policy

Configuring Health Policies



Displaying the network policies

Configuring Health Policies



Viewing NAP Enforcement for a network policy

Configuring Health Policies

NAP enforcement settings:

- **NAP DHCP-compliant**: Allow full network access.
- **NAP DHCP-noncompliant**: Allow limited access.
- **NAP DHCP nonNAPcapable properties**: Allow full network access.

Configuring Isolation and Remediation

- If a computer is noncompliant, it should be isolated from production network.
- When you configure NAP, you can configure either a monitor only policy or an isolation policy.

Configuring Isolation and Remediation

Remediation servers typically consist of:

- DHCP servers to provide IP configuration
- Naming servers including DNS servers and WINS servers
- Active Directory domain controllers (read-only domain controllers are recommended to minimize security risks)
- Internet proxy servers so that noncompliant NAP clients can access the Internet

Configuring Isolation and Remediation

Remediation servers typically consist of (continued):

- HRAs so that noncompliant NAP clients can obtain a health certificate for the IPsec enforcement method
- Web server that contains the troubleshooting URL server, so users can access information on compliance
- Anti-virus/anti-malware servers to retrieve updated anti-virus/anti-malware updates
- Software update servers so that clients can get Windows updates

Configuring NAP Client Settings

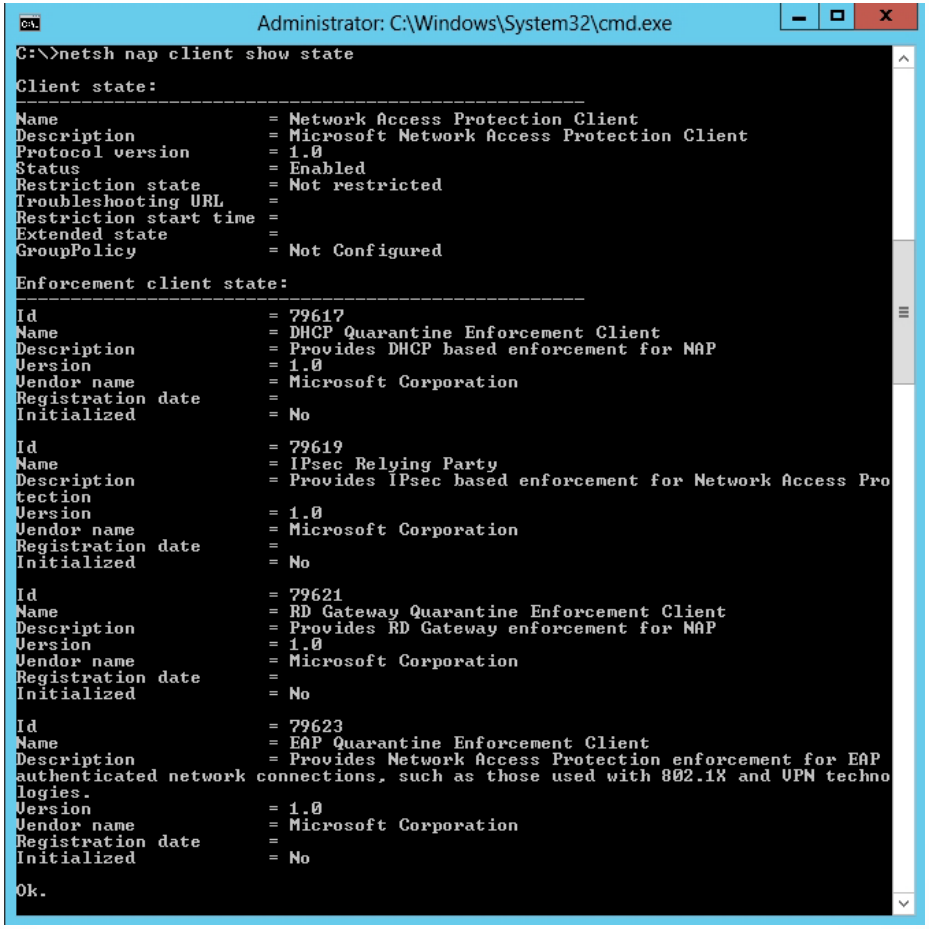
- You can use the Enable Security Center in the Group Policy procedure to enable Security Center on NAP-capable clients using Group Policy.
- Some NAP deployments that use Windows Security Health Validator require Security Center.
- Open the Services console to start and set the startup type to Automatic in the Network Access Protection Agent service.

Configuring NAP Client Settings

To verify a client's configuration, run the following command:

```
netsh nap client show state
```

Configuring NAP Client Settings



Using the `netsh nap client show state` command

Lesson Summary

- Microsoft Network Access Protection (NAP) is software for controlling networked computers based on the host's health.
- NAP includes built-in enforcement methods that define the mechanisms that NAP can use, including DHCP, Internet Protocol Security (IPsec), VPN, 802.1, and more.
- System Health Agents (SHAs) are components that report on one or more elements of the health of a NAP client.
- Each SHA creates a Statement of Health (SoH) that transmits to the NAP Agent. Each SHA generates a new Statement of Health whenever the status is updated.
- NAP Agent maintains information about the health of the NAP client computer and transmits information between the NAP enforcement clients and the SHAs.

Lesson Summary

- System Health Validators (SHVs) settings define requirements for client computers that connect to your computer.
- Health policies consist of one or more system health validators and other settings that enable you to define client computer configuration requirements for NAP-capable computers.
- Typically, you use a monitor-only policy when you first implement NAP to test the implementation so that you can verify which computers are blocked and which are granted access to the production network by viewing the security logs in the Event Viewer on the NAP server.
- A remediation server group and troubleshooting URL will be available to users if they fail the compliance check.
- For clients to use NAP, they must have Security Center enabled and have the NAP Agent service running.