

Lesson 14: Configuring Network Access Protection (NAP)

MOAC 70-411: Administering
Windows Server 2012

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

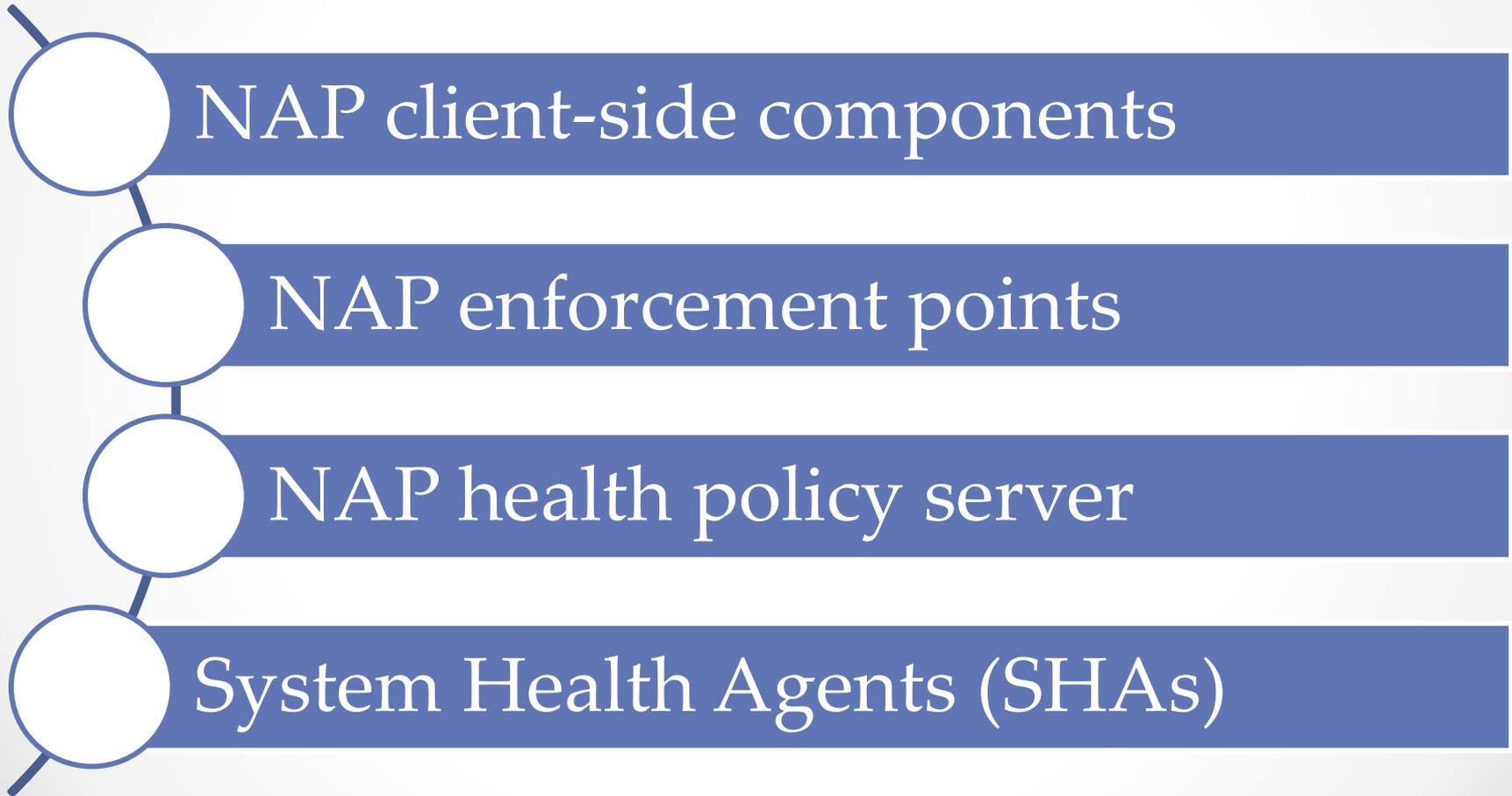
IPsec

VPN

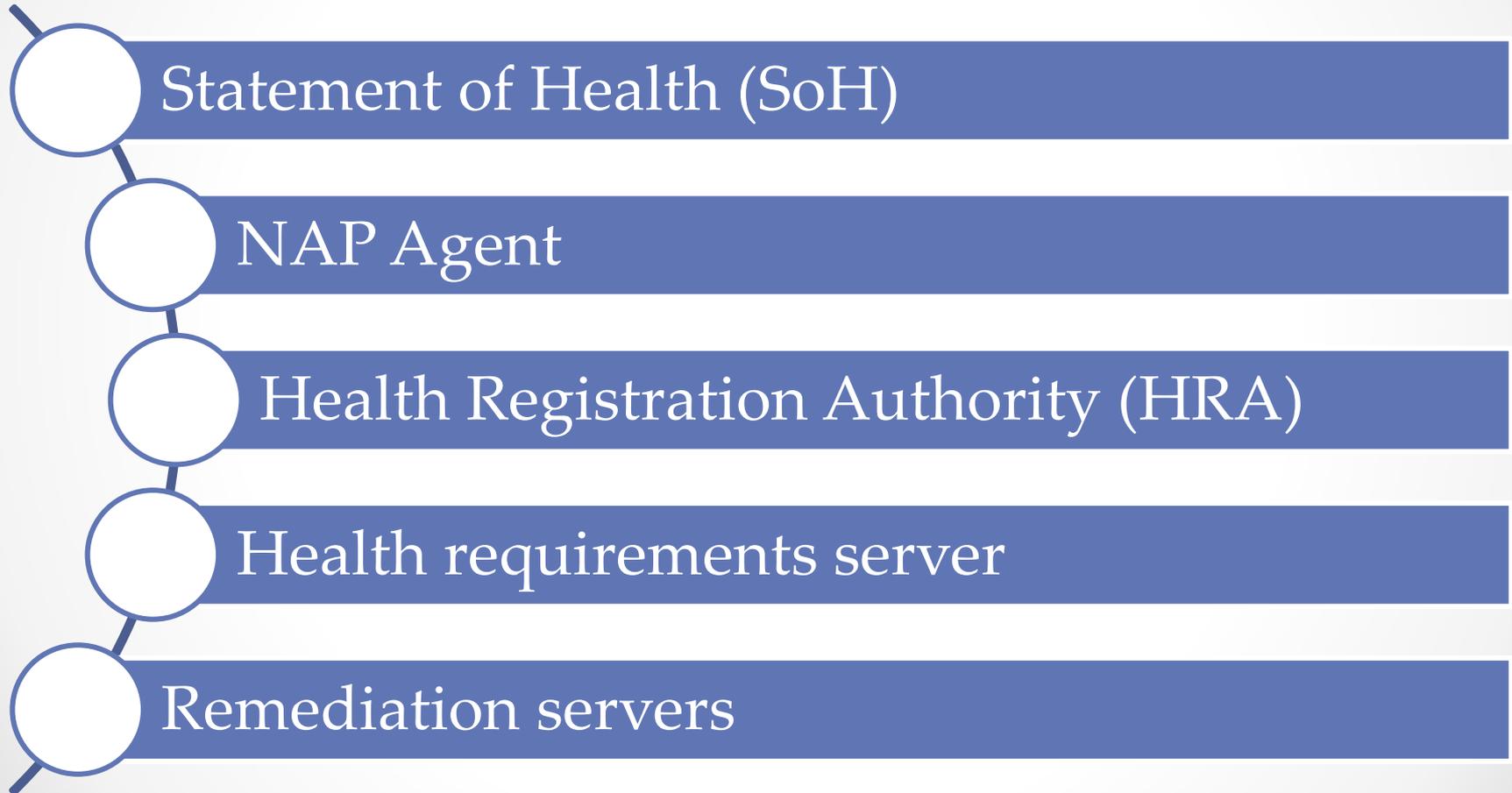
802.1x

Remote Desktop
Gateway (RD
Gateway)

NAP Architecture Components



NAP Architecture Components (cont.)



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.

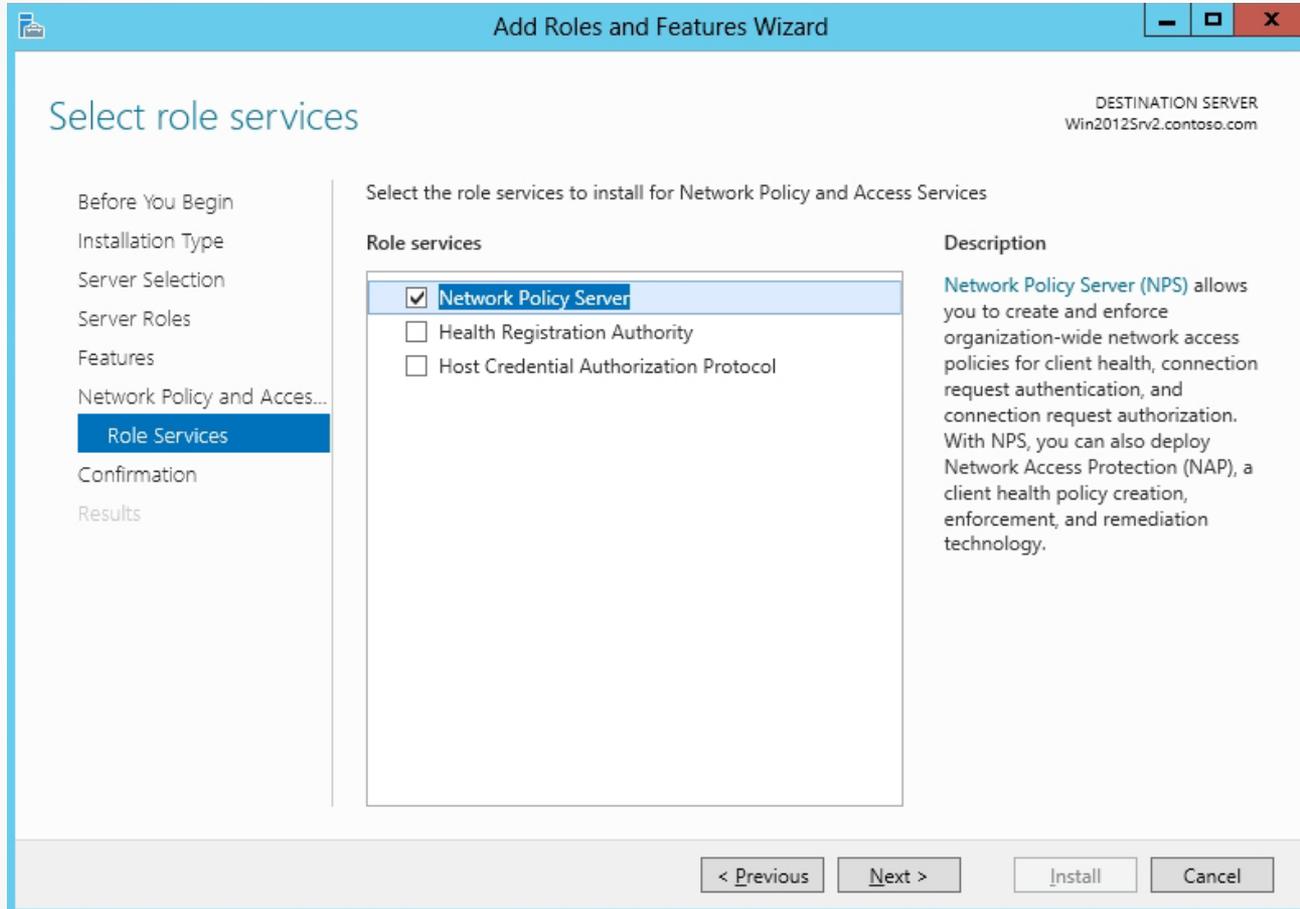
NAP Connection Process

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

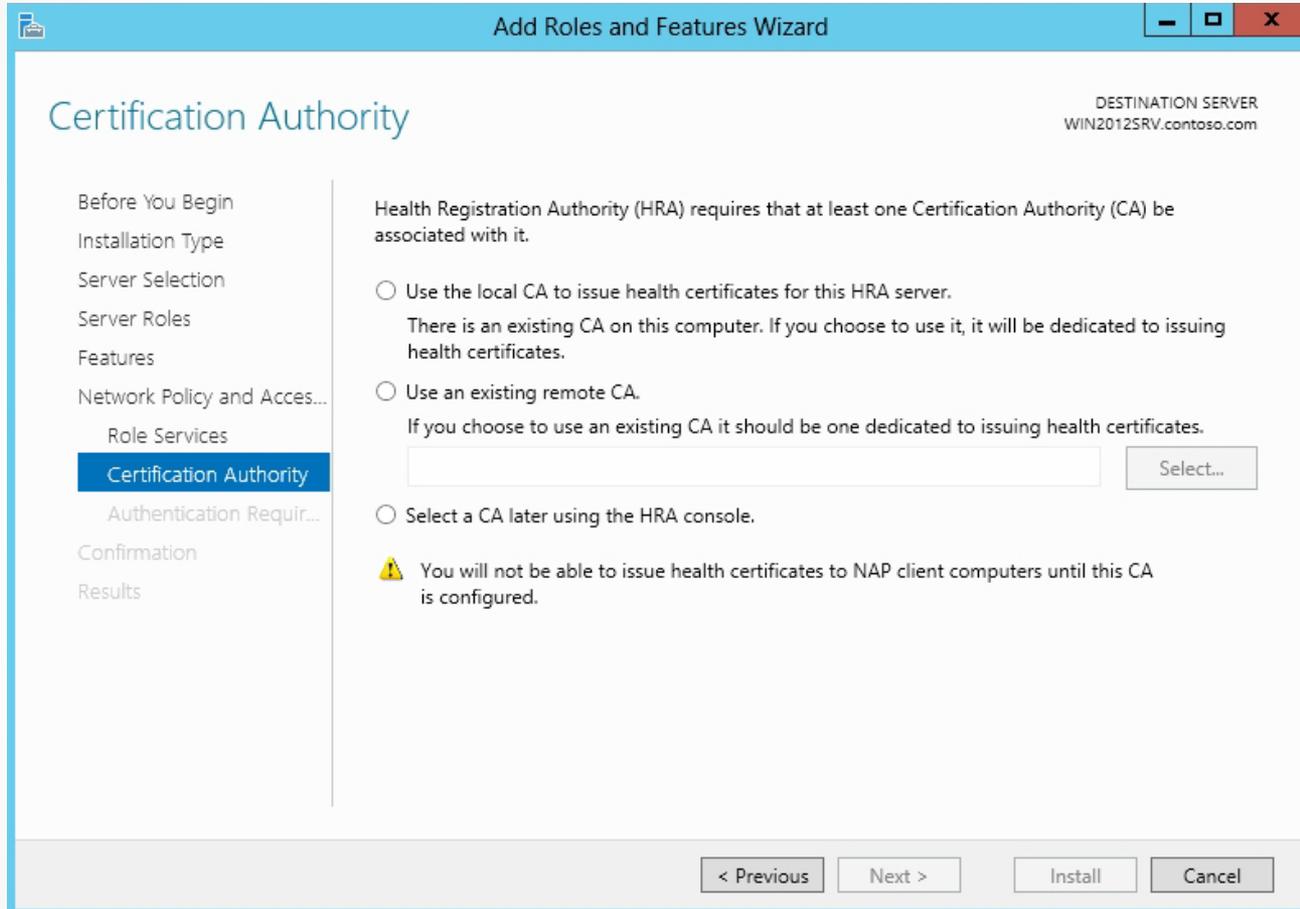
- Because NAP is offered through NPS, the installation is similar to installing NPS (discussed in Lesson 12).
- However, you want to add HRA, which is used to issue health certificates to NAP client computers that are compliant with network health requirements.
- For HRA to function, you need to have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

Install Network Policy Server



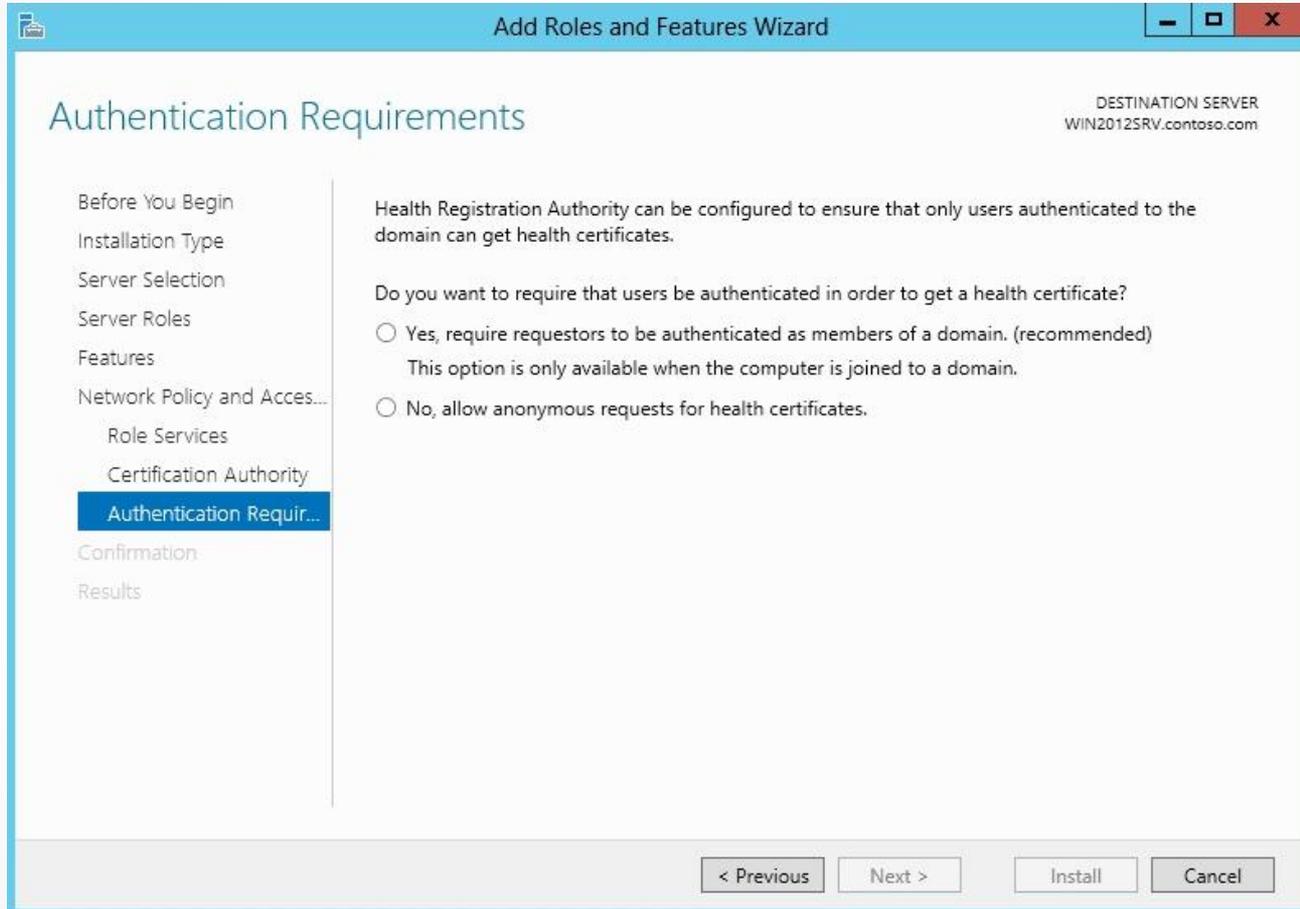
Selecting the role services

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:

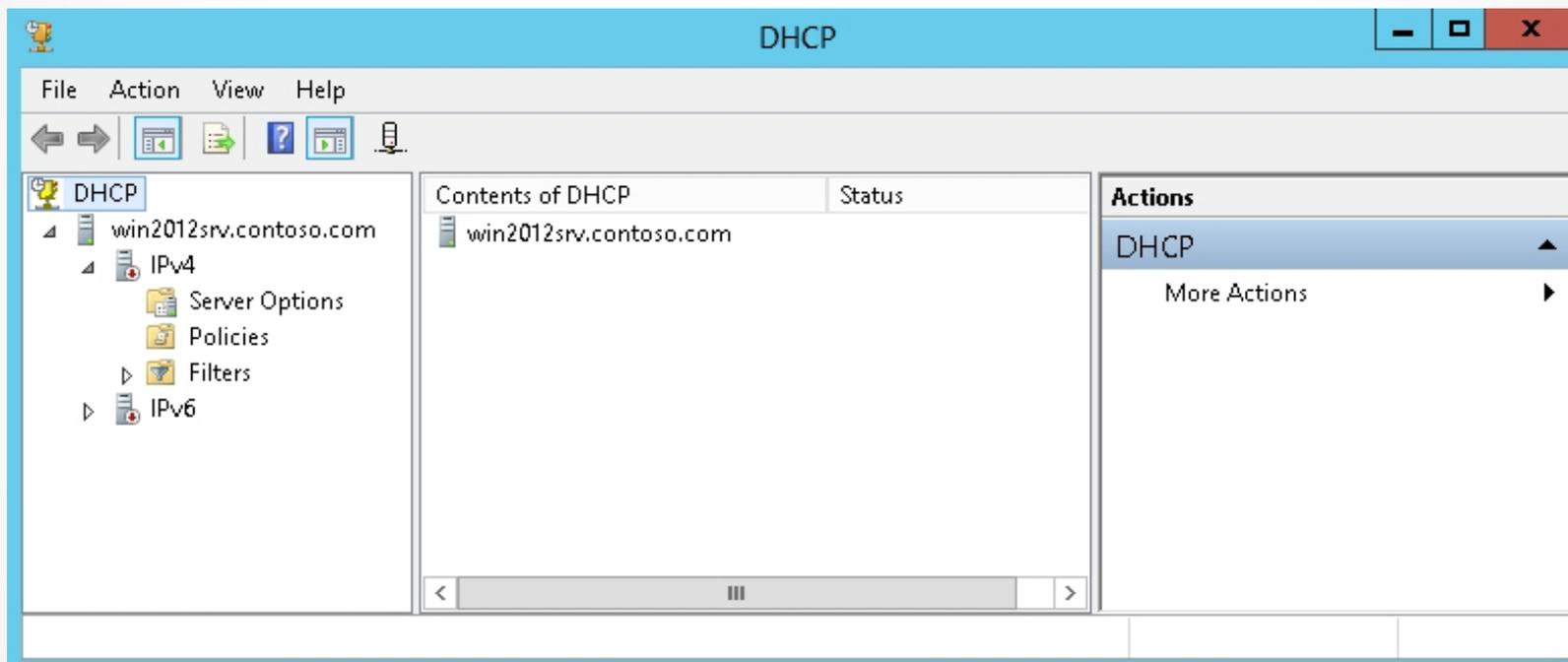
- DHCP Router option is set to 0.0.0.0 so noncompliant computers do not have a configured default gateway.
- Subnet mask is set to 255.255.255.255 so that there are no routes to the attached subnet.

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 servers, 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

New Scope Wizard

Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

Defining the scope name

Configure the DHCP Server

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

Specifying the IP address range

Configure the DHCP Server

New Scope Wizard

Lease Duration
The lease duration specifies how long a client can use an IP address from this scope. 

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:	Hours:	Minutes:
<input type="text" value="0"/>	<input type="text" value="8"/>	<input type="text" value="0"/>

< Back Next > Cancel

Specifying the lease duration

Configure the DHCP Server

New Scope Wizard

Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

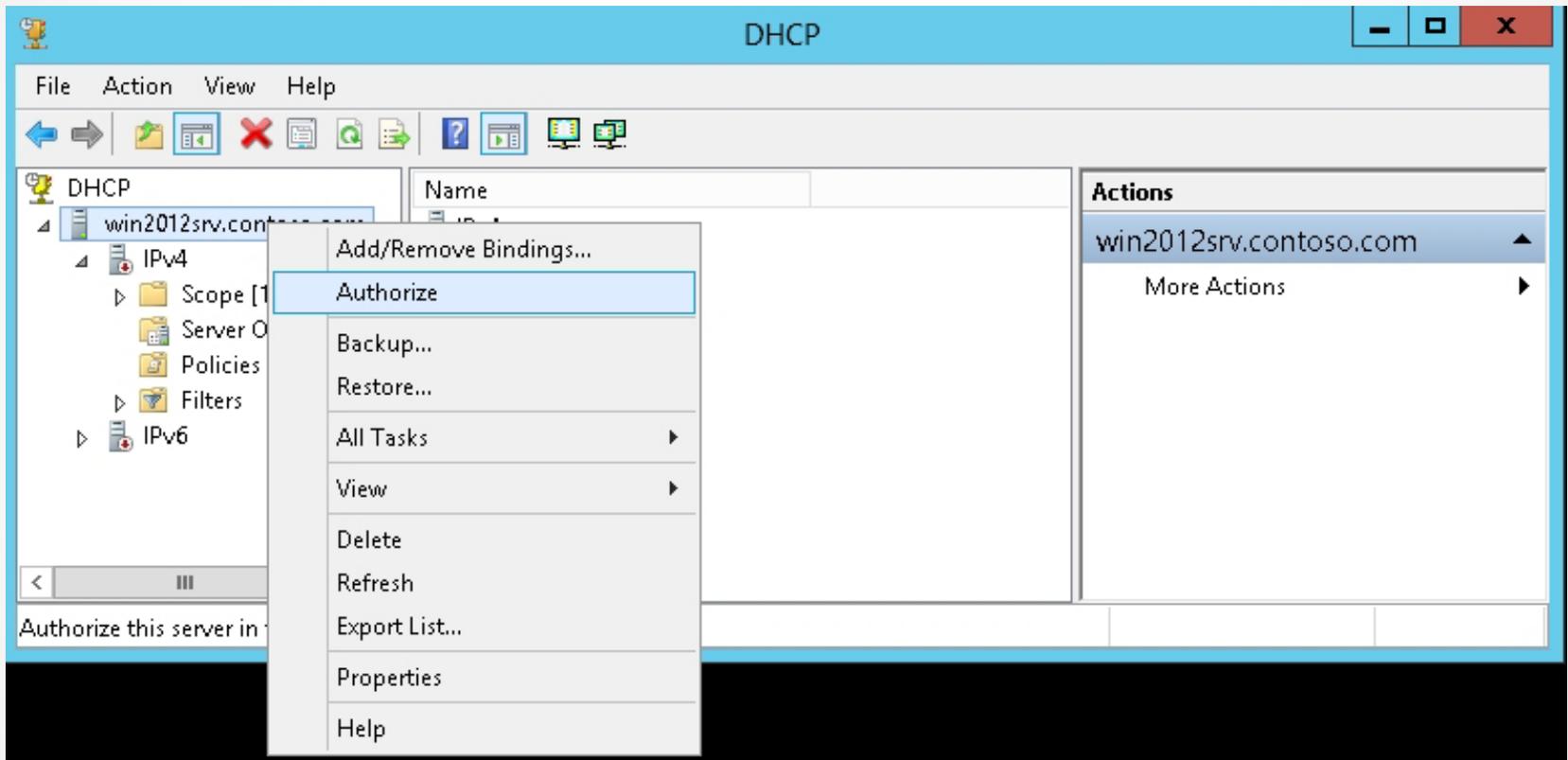
IP address:

<input type="text" value=" . . ."/>	Add
	Remove
	Up
	Down

< Back Next > Cancel

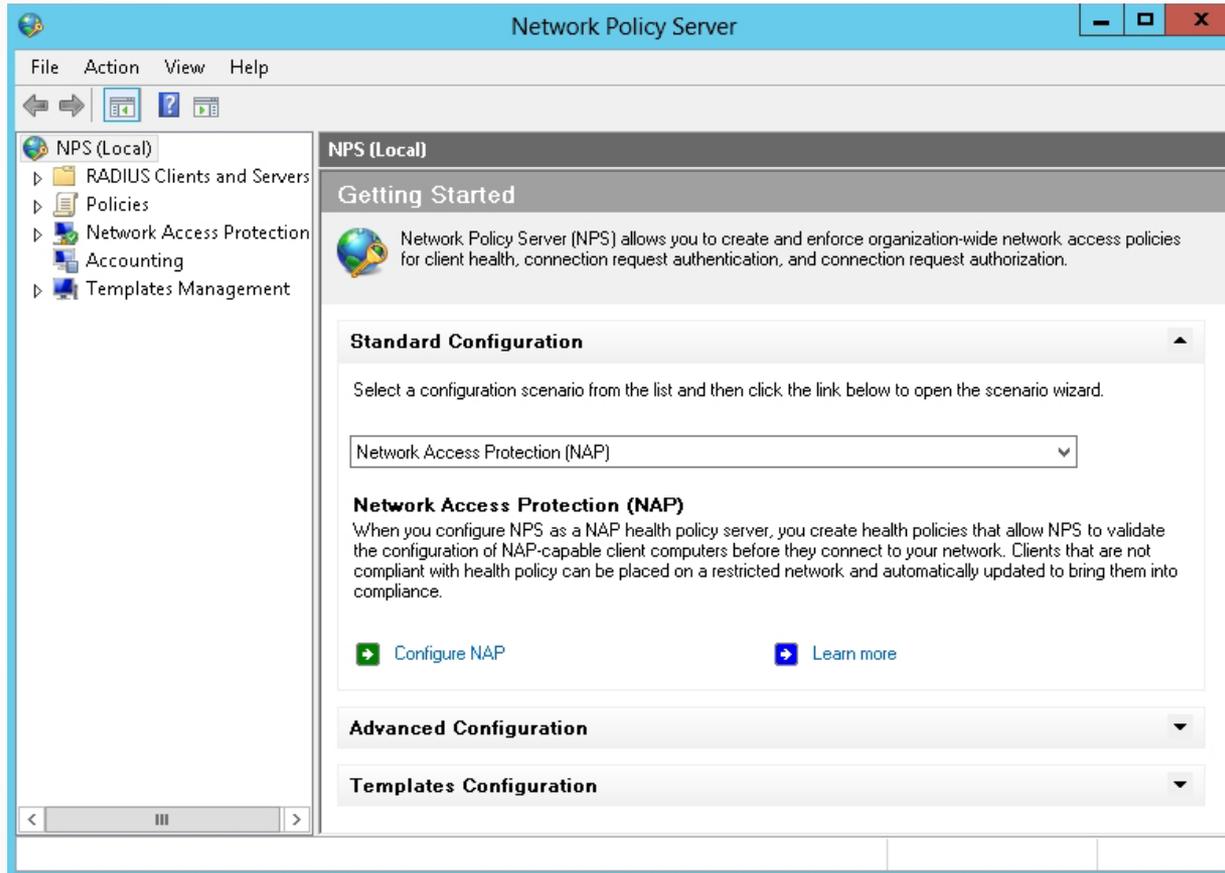
Defining the default gateway

Configure the DHCP Server



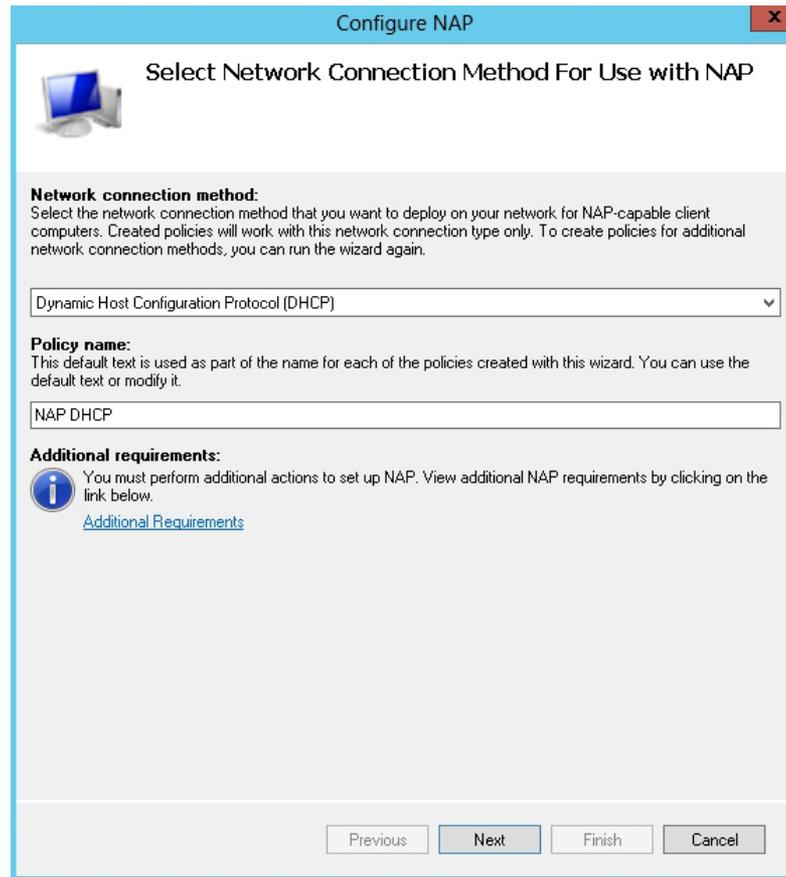
Authorizing the DHCP server

Configure NAP for DHCP Server



Starting the Network Policy Server console

Configure NAP for DHCP Server



The screenshot shows a window titled "Configure NAP" with a close button in the top right corner. The main heading is "Select Network Connection Method For Use with NAP" next to a computer icon. Below this, there is a section for "Network connection method:" with a dropdown menu currently set to "Dynamic Host Configuration Protocol (DHCP)". A "Policy name:" section contains a text box with "NAP DHCP". An "Additional requirements:" section features an information icon and a link to "Additional Requirements". At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

Configure NAP

Select Network Connection Method For Use with NAP

Network connection method:
Select the network connection method that you want to deploy on your network for NAP-capable client computers. Created policies will work with this network connection type only. To create policies for additional network connection methods, you can run the wizard again.

Dynamic Host Configuration Protocol (DHCP)

Policy name:
This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it.

NAP DHCP

Additional requirements:
You must perform additional actions to set up NAP. View additional NAP requirements by clicking on the link below.
[Additional Requirements](#)

Previous Next Finish Cancel

Selecting the network connection method

Configure NAP for DHCP Server



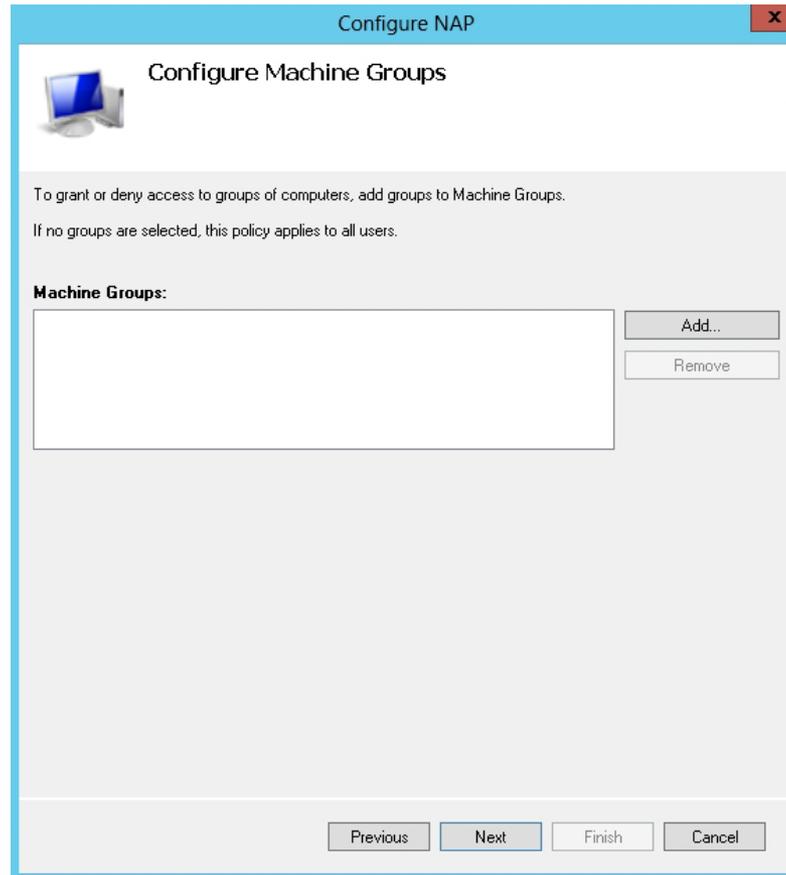
Specifying NAP enforcement servers running DHCP server

Configure NAP for DHCP Server



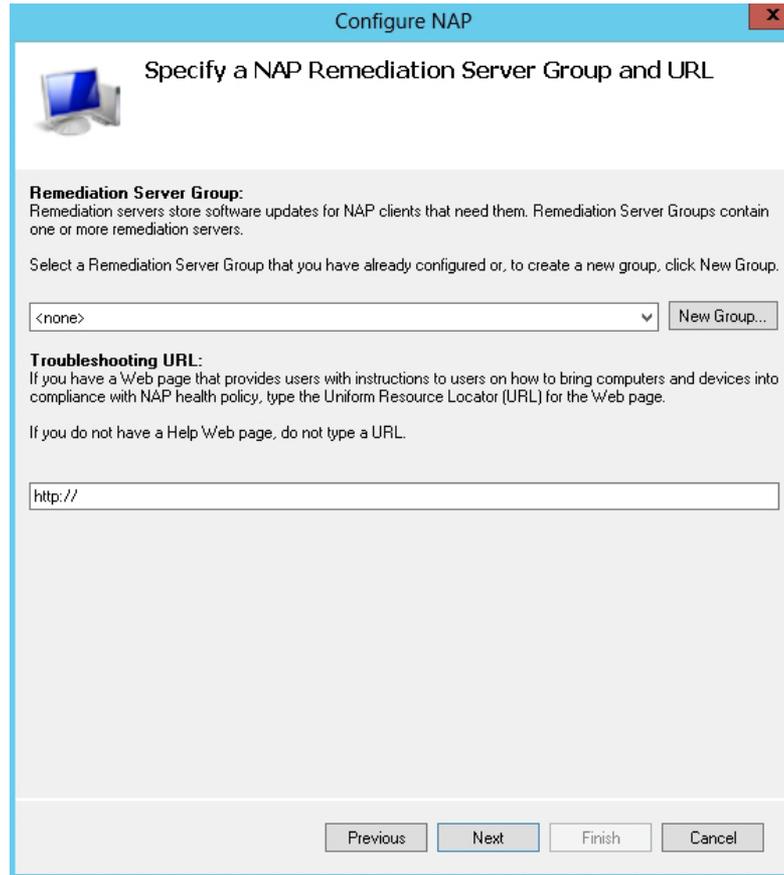
Specifying the DHCP scopes to apply to NAP

Configure NAP for DHCP Server



Specifying the computer groups that NAP will apply to

Configure NAP for DHCP Server



The screenshot shows a window titled "Configure NAP" with a close button in the top right corner. The main heading is "Specify a NAP Remediation Server Group and URL" next to a computer icon. Below this, there are two sections: "Remediation Server Group" and "Troubleshooting URL".

Remediation Server Group:
Remediation servers store software updates for NAP clients that need them. Remediation Server Groups contain one or more remediation servers.
Select a Remediation Server Group that you have already configured or, to create a new group, click New Group.

A dropdown menu shows "<none>" and a "New Group..." button is to its right.

Troubleshooting URL:
If you have a Web page that provides users with instructions to users on how to bring computers and devices into compliance with NAP health policy, type the Uniform Resource Locator (URL) for the Web page.
If you do not have a Help Web page, do not type a URL.

A text input field contains "http://".

At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

Specifying the NAP Remediation Server group and URL

Configure NAP for DHCP Server

New Remediation Server Group

Select an existing template:

Group Name:

Remediation Servers:

DNS Name / IP Address	Friendly Name
-----------------------	---------------

Add...
Edit...
Remove

OK Cancel

Adding computers to the Remediation Server group

Configure NAP for DHCP Server



The screenshot shows a Windows wizard window titled "Configure NAP" with a close button (X) in the top right corner. The main heading is "Define NAP Health Policy" with a computer icon to the left. Below the heading, a text box explains: "The installed System Health Validators are listed below. Select only the System Health Validators that you want to enforce with this health policy." A table lists the validators, with "Windows Security Health Validator" selected. Below the table, there is a checkbox for "Enable auto-remediation of client computers" which is checked, followed by explanatory text. At the bottom, there are radio buttons for "Network access restrictions for NAP-ineligible client computers:", with "Deny full network access to NAP-ineligible client computers. Allow access to a restricted network only." selected. The bottom of the window contains four buttons: "Previous", "Next", "Finish", and "Cancel".

Configure NAP

Define NAP Health Policy

The installed System Health Validators are listed below. Select only the System Health Validators that you want to enforce with this health policy.

Name
<input checked="" type="checkbox"/> Windows Security Health Validator

Enable auto-remediation of client computers

If selected, NAP-capable client computers that are denied full access to the network because they are not compliant with health policy can obtain software updates from remediation servers.

If not selected, noncompliant NAP-capable client computers are not automatically updated and cannot gain full network access until they are manually updated.

Network access restrictions for NAP-ineligible client computers:

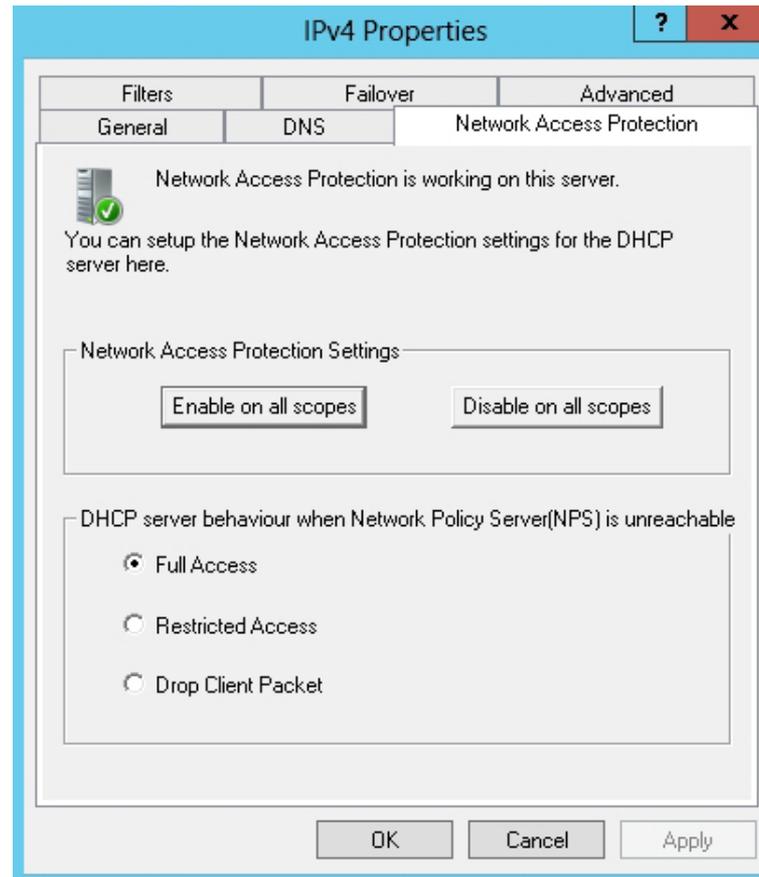
Deny full network access to NAP-ineligible client computers. Allow access to a restricted network only.

Allow full network access to NAP-ineligible client computers.

Previous Next Finish Cancel

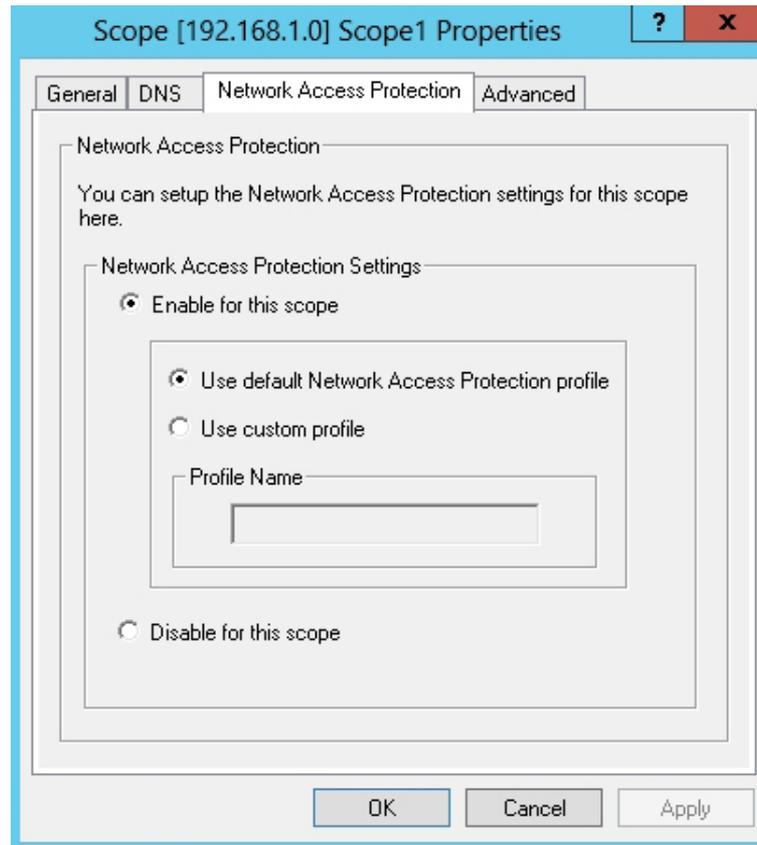
Defining NAP Health Policy

Enable NAP on All DHCP Scopes



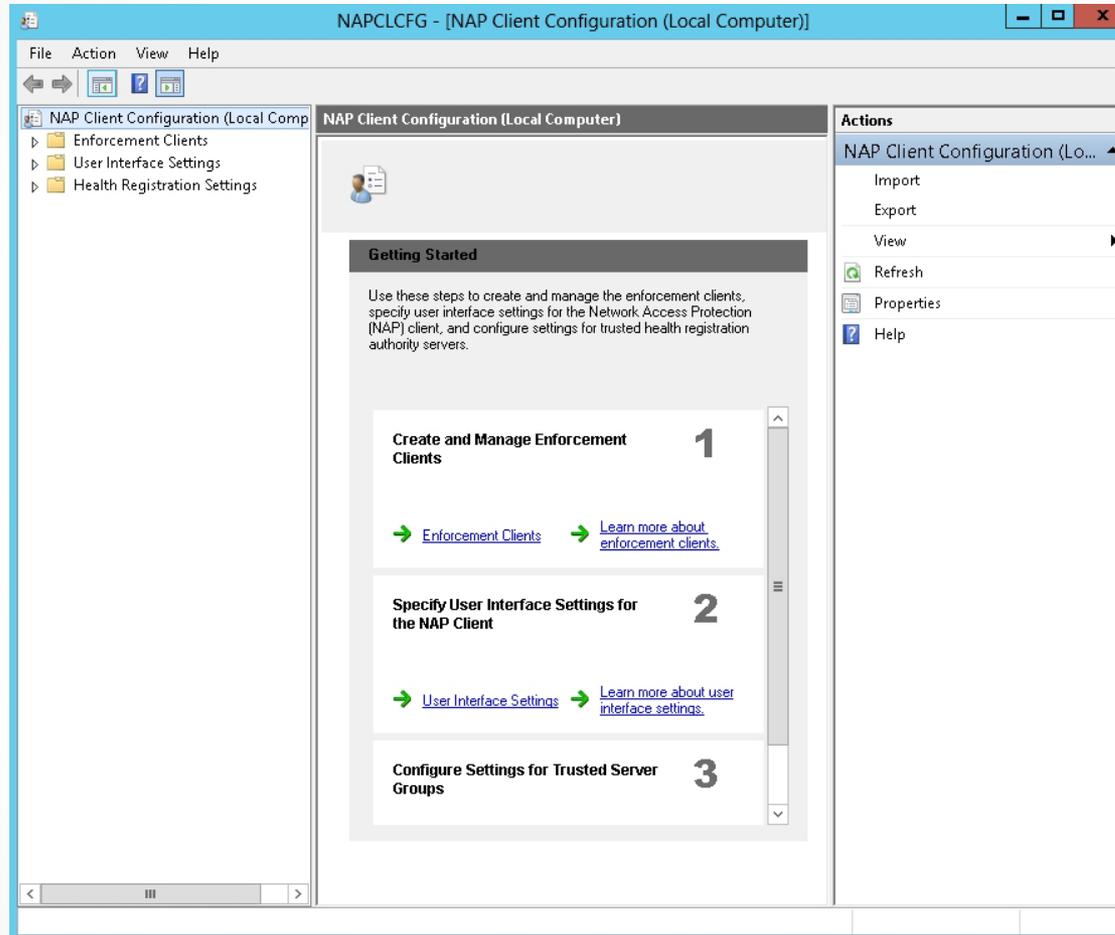
Enabling NAP for all DHCP scopes

Enable NAP on an Individual DHCP Scope



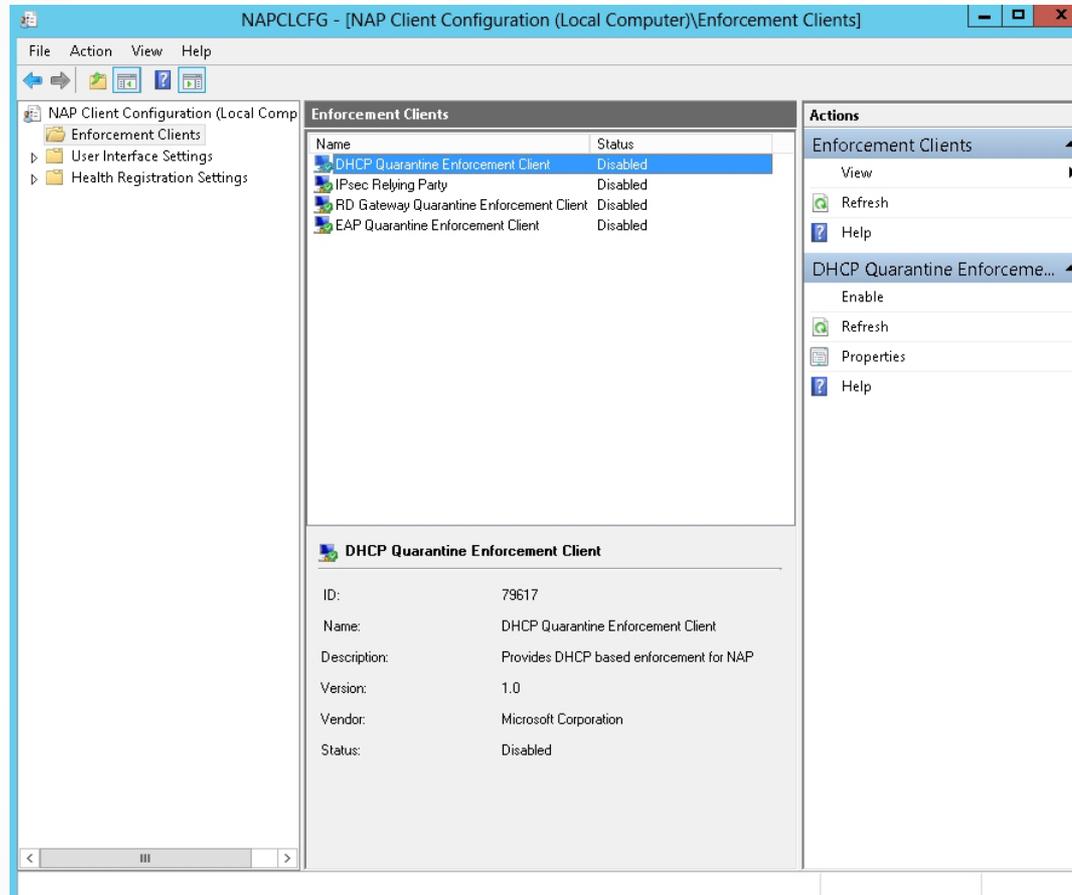
Enabling NAP for individual DHCP scopes

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



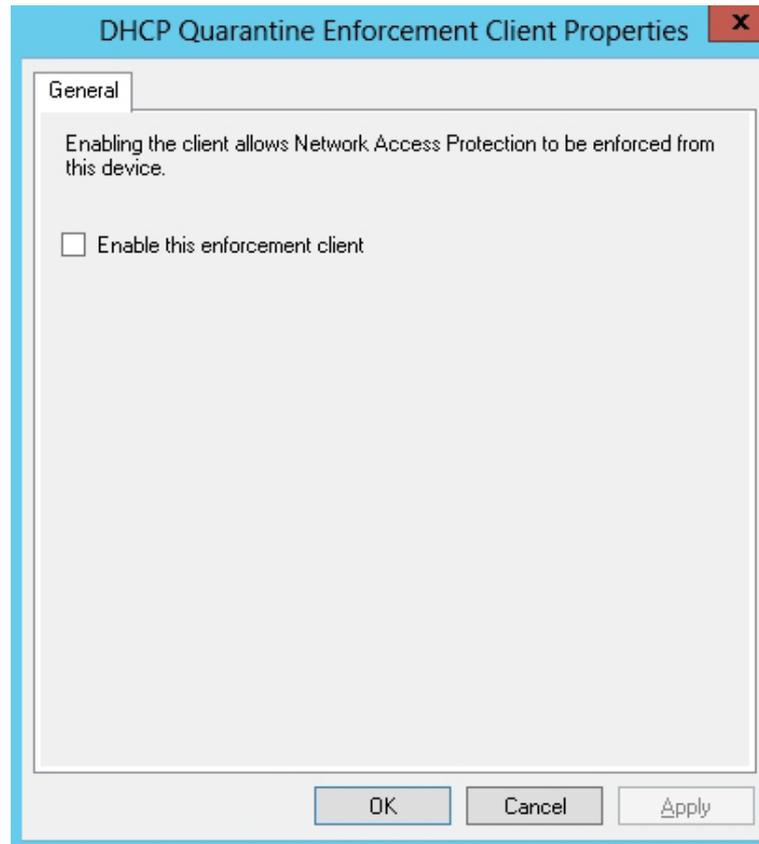
Opening the NAP Client Configuration console

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 servers, 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

Configure NAP

Select Network Connection Method For Use with NAP

Network connection method:
Select the network connection method that you want to deploy on your network for NAP-capable client computers. Created policies will work with this network connection type only. To create policies for additional network connection methods, you can run the wizard again.

Virtual Private Network (VPN)

Policy name:
This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it.

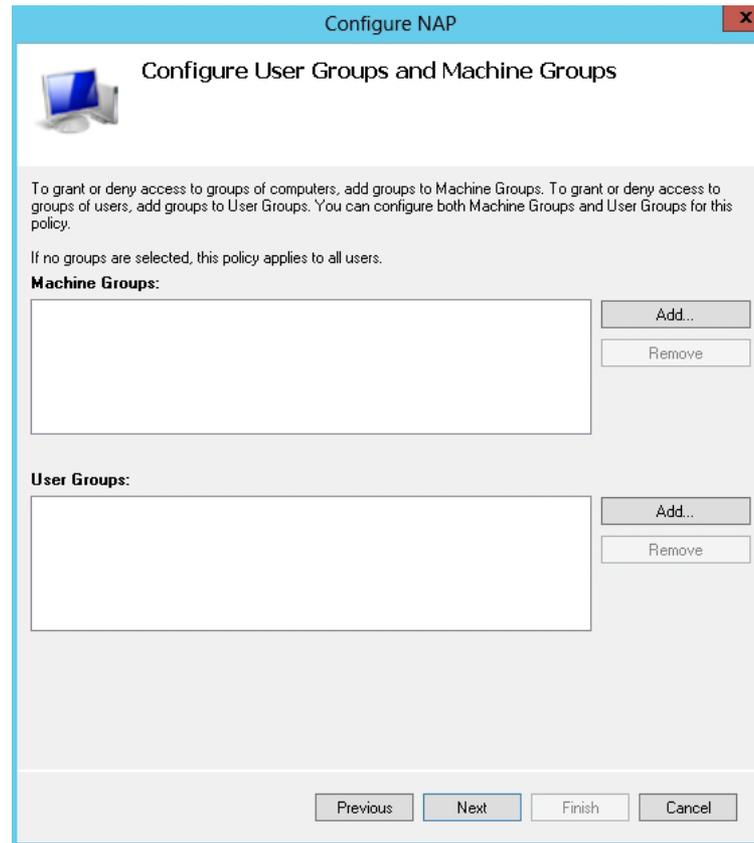
NAP VPN

Additional requirements:
You must perform additional actions to set up NAP. View additional NAP requirements by clicking on the link below.
[Additional Requirements](#)

Previous Next Finish Cancel

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

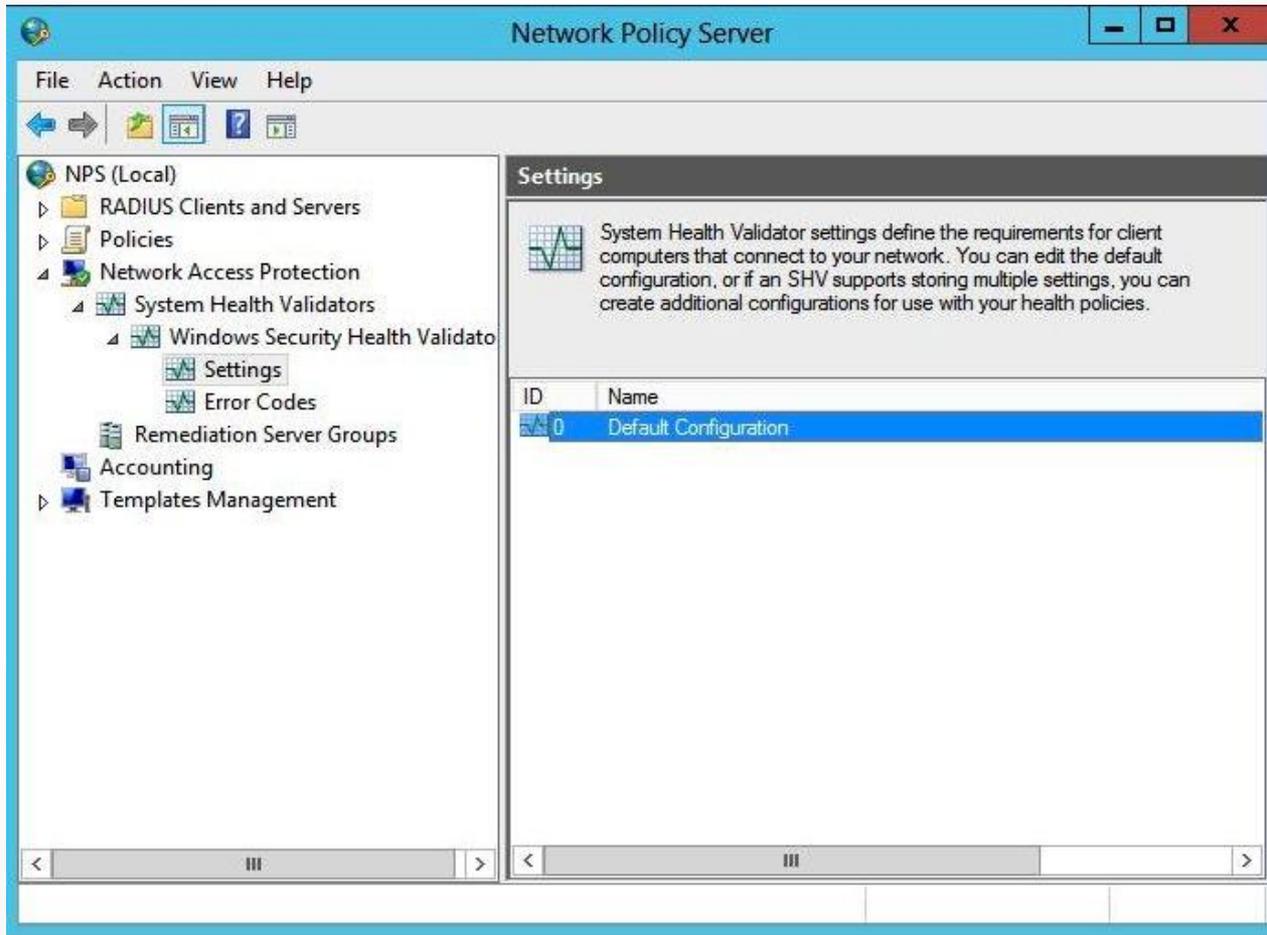


Configuring an authentication method for NAP

System Health Validators

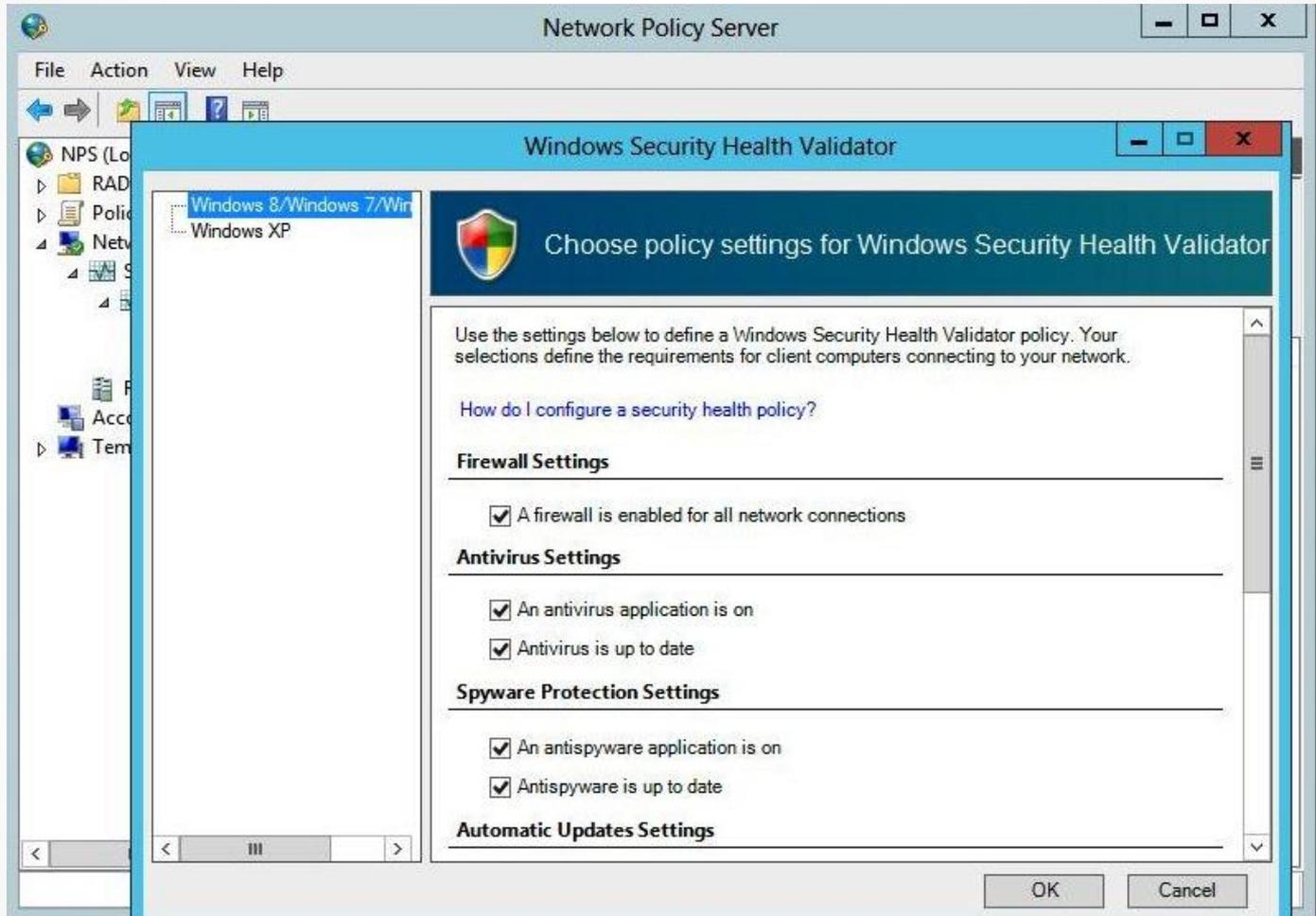
- **System Health Validators (SHVs)** settings define the requirements for client computers that connect to your network.
- You configure SHVs using the Network Policy Server console.
- Windows 8 includes a Windows Security Health Validator SHA that monitors the Windows Security Center settings.
- Windows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

NAP DHCP Compliant Properties [X]

Settings

Configure health policy settings. To enforce the health policy, add it to the Health Policies condition of one or more network policies.

Select an existing template:

Policy name:
NAP DHCP Compliant

Client SHV checks:
Client passes all SHV checks

SHVs used in this health policy:

	Name	Setting
<input checked="" type="checkbox"/>	Windows Security Health Validator	Default Configuration

OK Cancel Apply

NAP DHCP Noncompliant Properties [X]

Settings

Configure health policy settings. To enforce the health policy, add it to the Health Policies condition of one or more network policies.

Select an existing template:

Policy name:
NAP DHCP Noncompliant

Client SHV checks:
Client fails one or more SHV checks

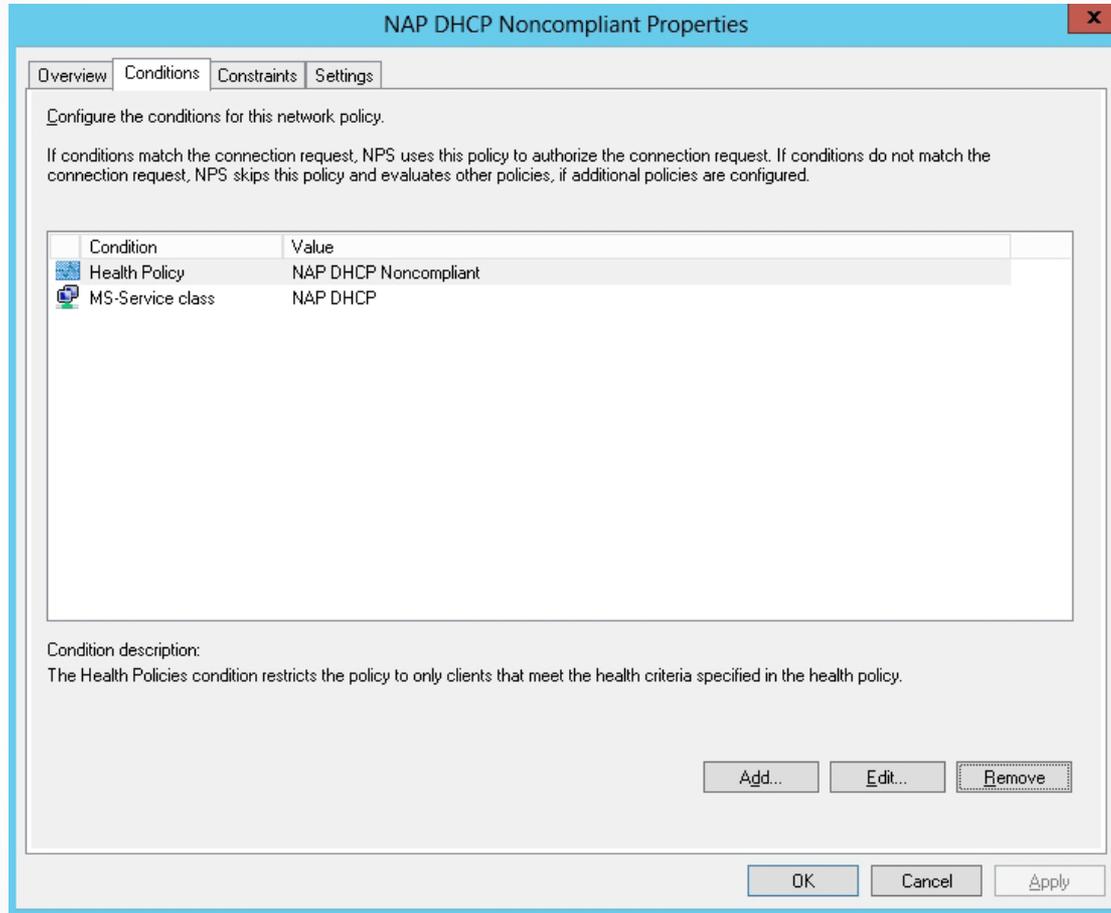
SHVs used in this health policy:

	Name	Setting
<input checked="" type="checkbox"/>	Windows Security Health Validator	Default Configuration

OK Cancel Apply

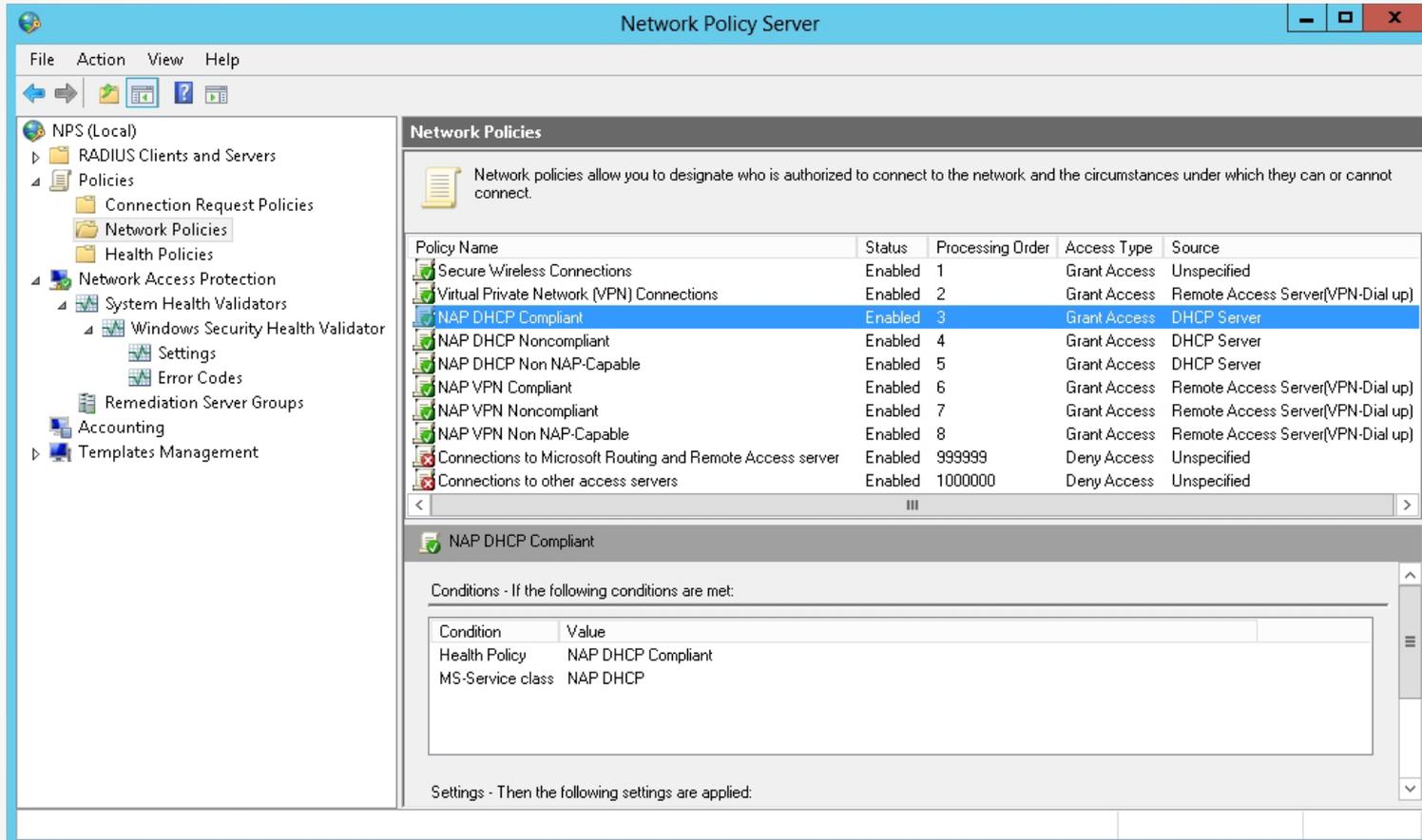
Viewing the health policies

Configuring Health Policies



Displaying the conditions of a health policy

Configuring Health Policies



The screenshot displays the Network Policy Server (NPS) console. The left-hand pane shows the navigation tree with 'Network Policies' selected. The main pane shows a list of network policies with the following data:

Policy Name	Status	Processing Order	Access Type	Source
Secure Wireless Connections	Enabled	1	Grant Access	Unspecified
Virtual Private Network (VPN) Connections	Enabled	2	Grant Access	Remote Access Server(VPN-Dial up)
NAP DHCP Compliant	Enabled	3	Grant Access	DHCP Server
NAP DHCP Noncompliant	Enabled	4	Grant Access	DHCP Server
NAP DHCP Non NAP-Capable	Enabled	5	Grant Access	DHCP Server
NAP VPN Compliant	Enabled	6	Grant Access	Remote Access Server(VPN-Dial up)
NAP VPN Noncompliant	Enabled	7	Grant Access	Remote Access Server(VPN-Dial up)
NAP VPN Non NAP-Capable	Enabled	8	Grant Access	Remote Access Server(VPN-Dial up)
Connections to Microsoft Routing and Remote Access server	Enabled	999999	Deny Access	Unspecified
Connections to other access servers	Enabled	1000000	Deny Access	Unspecified

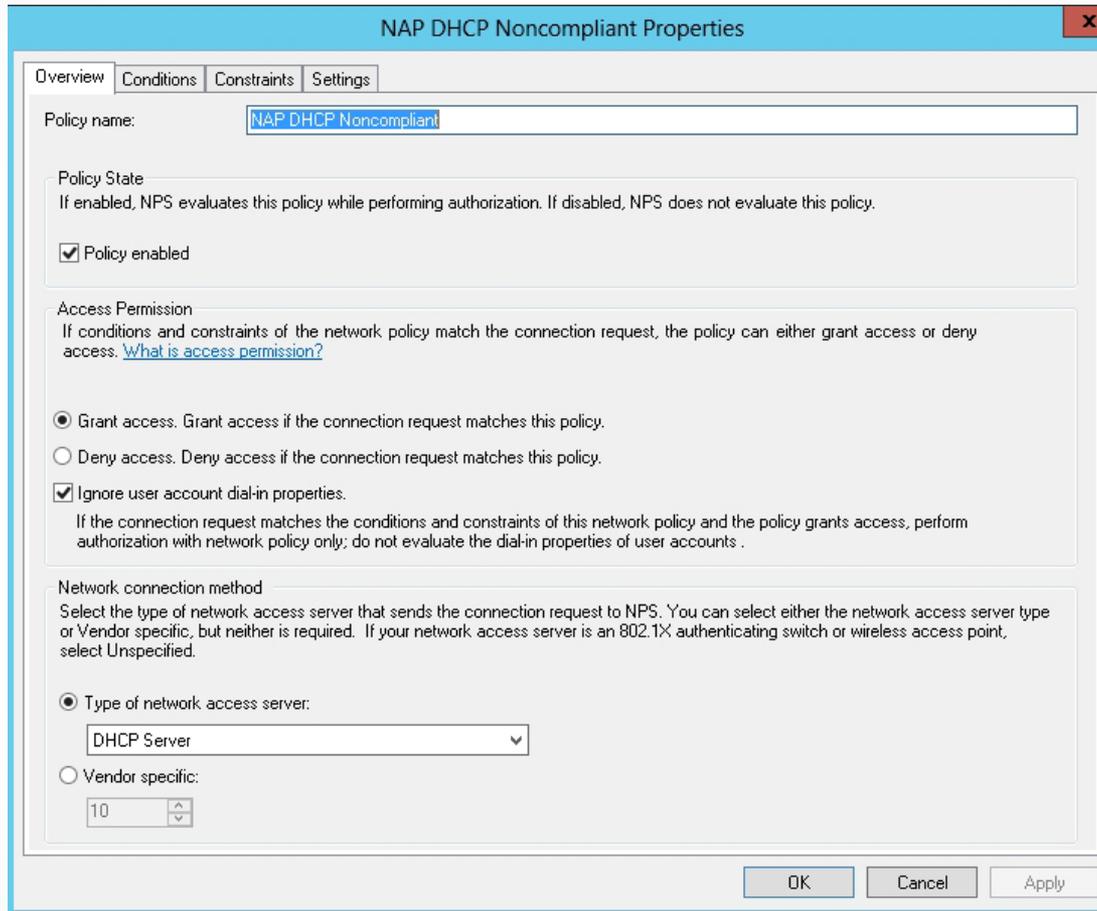
Below the list, the configuration for the selected 'NAP DHCP Compliant' policy is shown. It includes a section for 'Conditions - If the following conditions are met:' with the following table:

Condition	Value
Health Policy	NAP DHCP Compliant
MS-Service class	NAP DHCP

There is also a section for 'Settings - Then the following settings are applied:' which is currently empty.

Displaying the network policies

Configuring Health Policies



NAP DHCP Noncompliant Properties

Overview | Conditions | Constraints | Settings

Policy name:

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:

Vendor specific:

OK Cancel Apply

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

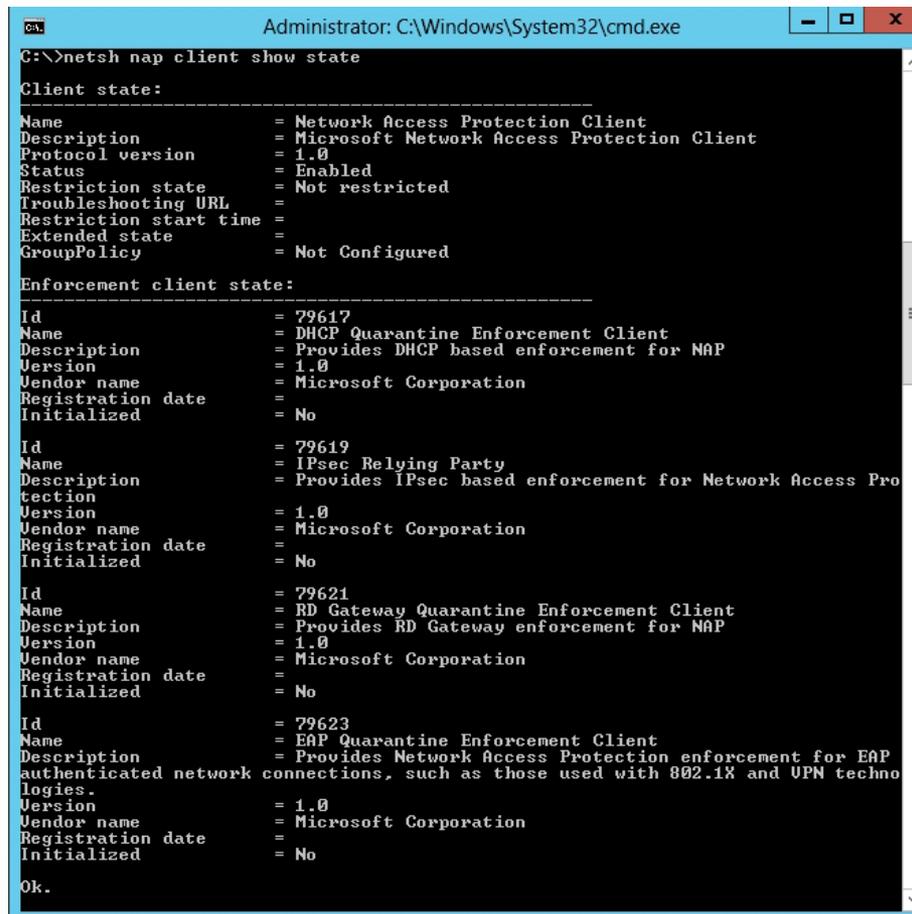
- You can use the Enable Security Center in the Group Policy procedure to enable Security Center on NAP-capable clients using Group Policy.
- Some NAP deployments that use Windows Security Health Validator require Security Center.
- Open the Services console to start and set the startup type to Automatic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



```
Administrator: C:\Windows\System32\cmd.exe
C:\>netsh nap client show state

Client state:
-----
Name = Network Access Protection Client
Description = Microsoft Network Access Protection Client
Protocol version = 1.0
Status = Enabled
Restriction state = Not restricted
Troubleshooting URL =
Restriction start time =
Extended state =
GroupPolicy = Not Configured

Enforcement client state:
-----
Id = 79617
Name = DHCP Quarantine Enforcement Client
Description = Provides DHCP based enforcement for NAP
Version = 1.0
Vendor name = Microsoft Corporation
Registration date =
Initialized = No

Id = 79619
Name = IPsec Relying Party
Description = Provides IPsec based enforcement for Network Access Protection
Version = 1.0
Vendor name = Microsoft Corporation
Registration date =
Initialized = No

Id = 79621
Name = RD Gateway Quarantine Enforcement Client
Description = Provides RD Gateway enforcement for NAP
Version = 1.0
Vendor name = Microsoft Corporation
Registration date =
Initialized = No

Id = 79623
Name = EAP Quarantine Enforcement Client
Description = Provides Network Access Protection enforcement for EAP authenticated network connections, such as those used with 802.1X and UPN technologies.
Version = 1.0
Vendor name = Microsoft Corporation
Registration date =
Initialized = No

Ok.
```

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.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.