Use Group Policy Filtering to create a DHCP enforcement policy for NAP - Part 2

How to use the NAP policy wizard to automatically create Network, Health, and Connection policies to control your network.

Thomas Shinder

Network Administration - *In the first part of this series, we introduced some basic knowledge about how NAP works, then installed DHCP and NPS services on the NAP policy server. In this section, I will show you how to use the NAP policy wizard to automatically create Network, Health, and Connection policies to control access to your network.*

Use the NAP Wizard to create an NAP DHCP enforcement policy

Now we can start the main part - create a NAP DHCP enforcement policy. After running the wizard, the wizard will create the following policies:

- Health Policies
- Connection Request Policies
- Network Policies
- Remediation Server Group policies

Let's take a closer look at each of these policies after finishing the wizard.

Open the **Network Policy Server** console from the **Administrative Tools** menu. From here, you will see the middle of the interface appear the page **Getting Started.** In the **Standard Configuration** section, select the **Network Access Protection (NAP) option** from the **Select configuration scenario from the list and then click the link below to open the wizard scenario** .

Click the **Configure NAP** link.

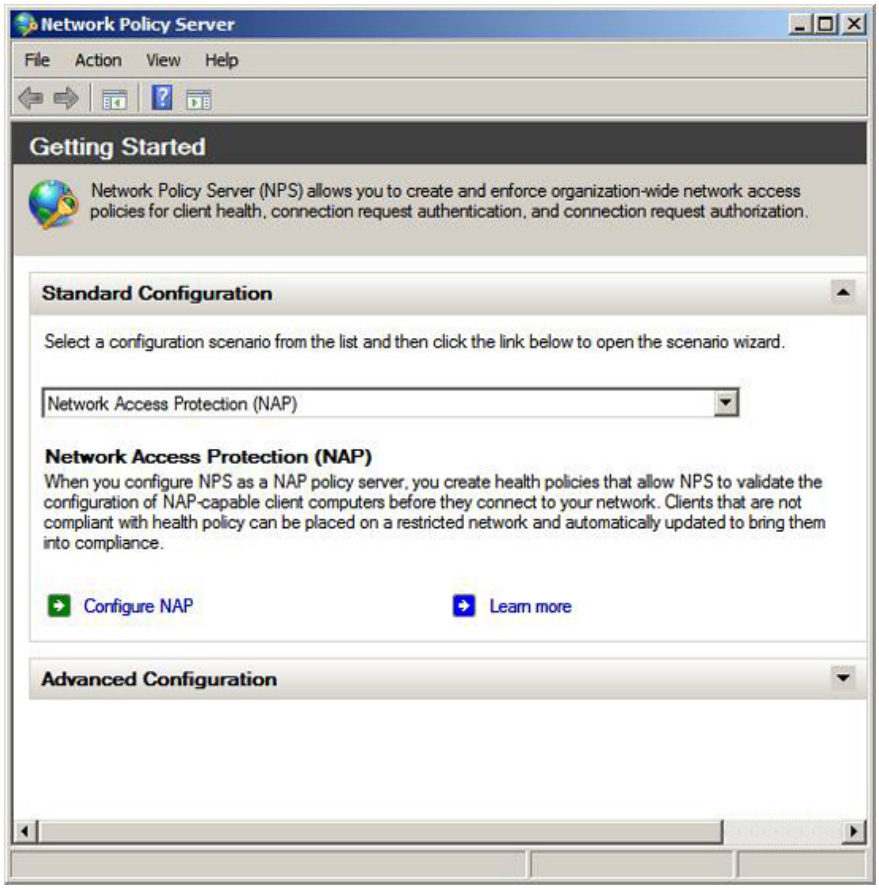

Figure 1

On the **Select Network Connection Method For Use page with NAP** , the **Network connection method section** , select the option **Dynamic Host Configuration Protocol (DHCP)** from the list. Remember, when using NAP, we have to choose an execution method and that's what we're doing here. The DHCP server becomes 'network access server' in this scenario and the DHCP server is responsible for the network access level that the NAP client has.

The **Policy name** text box will automatically be populated with **NAP DHCP,** the name (name) section will be appended to some of the policies created by the wizard. We will see this after finishing the NAP wizard.

Click **Next** .

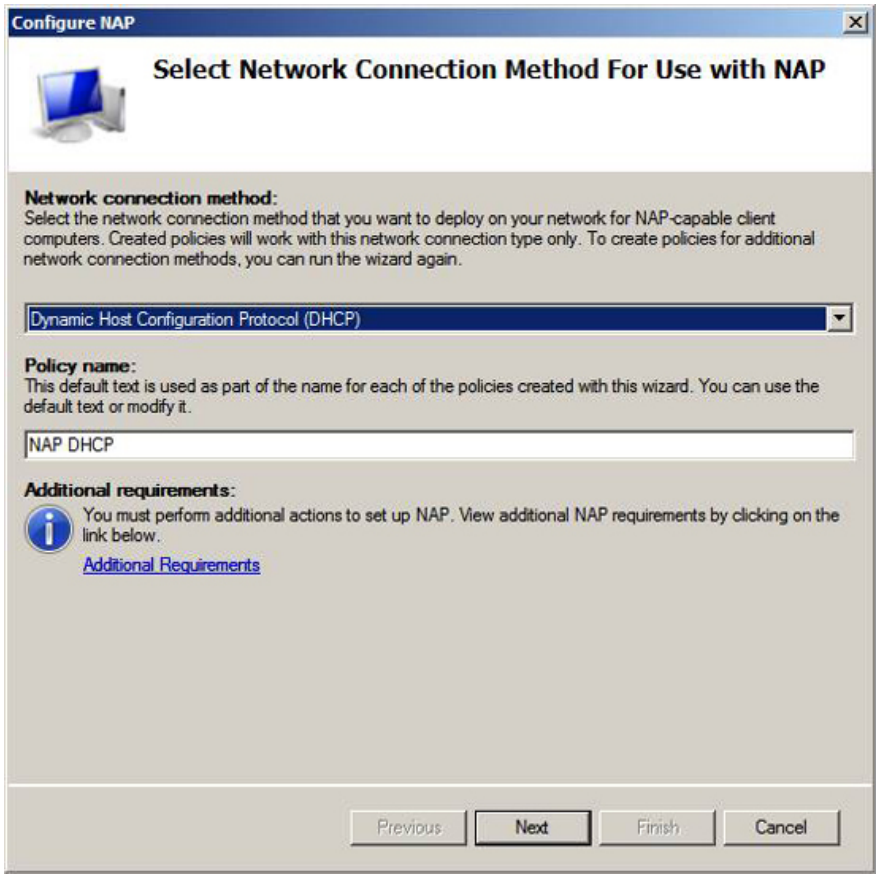

Figure 2

On the **Specify NAP Enforcement Server Running DHCP Server page** , you can include the IP address of the DHCP server that will be responsible for the network access server. Use this option when the DHCP server and NPS server configure NAP policies that are not on the same server.

If you want to add remote DHCP NAP enforcement servers, they must be configured as RADIUS clients, which means that you need to configure these as NPS servers. The difference here is that this NPS server does not configure NAP policy settings. They only authorize RADIUS requests to the NPS server that is configuring NAP policy settings. This configuration should be used in a large production environment, where the DHCP server and NAP server are both relatively busy. In addition, it is likely that there will be multiple DHCP servers in your company, while you want all to be able to communicate with the NAP policy server or servers.

In this example, the network on which we place DHCP and NPS servers is on the same computer, so we won't need to add remote DHCP servers to the list. Click **Next** .

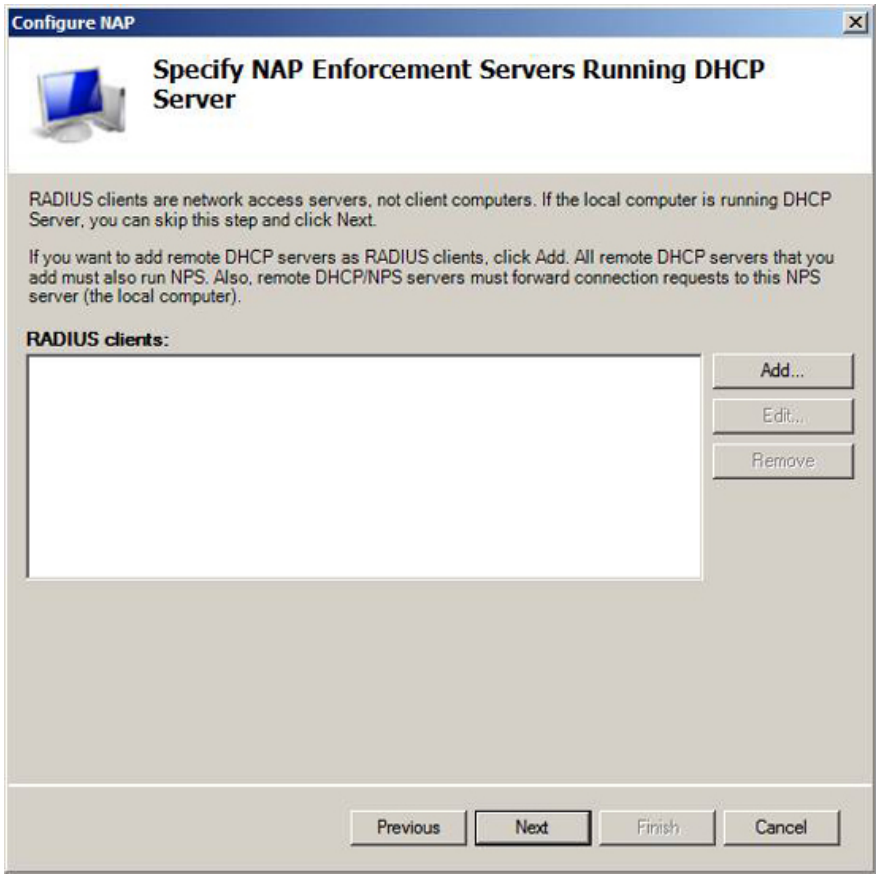

Figure 3

You have an option to enable NAP when using DHCP enforcement. If you do not want to use the NAP enforcement policy for all DHCP scopes, you can enter the scope in which you want the NAP policy to apply to the **Specify DHCP Scopes page.** In our example network, we want to enable NAP policy on all scopes, so we don't enter specific scopes on this page. Click **Next** .

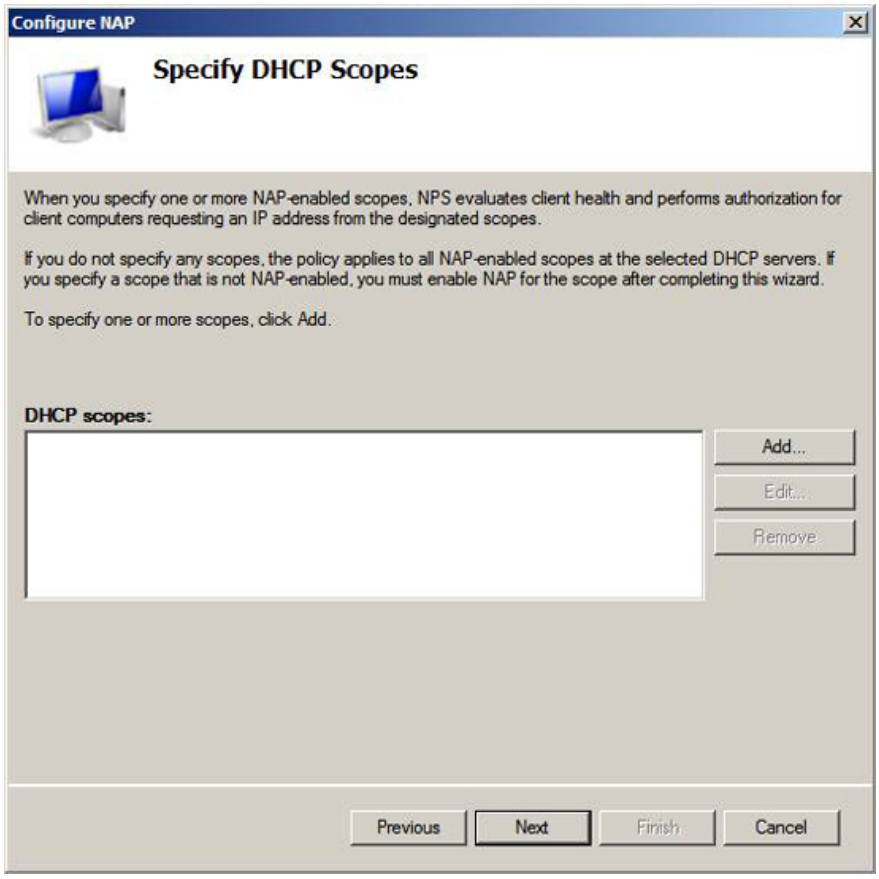

Figure 4

You can allow or deny access to certain user groups or computers in NAP policy. In this example, we apply policies to all machines and users. Click **Next.**

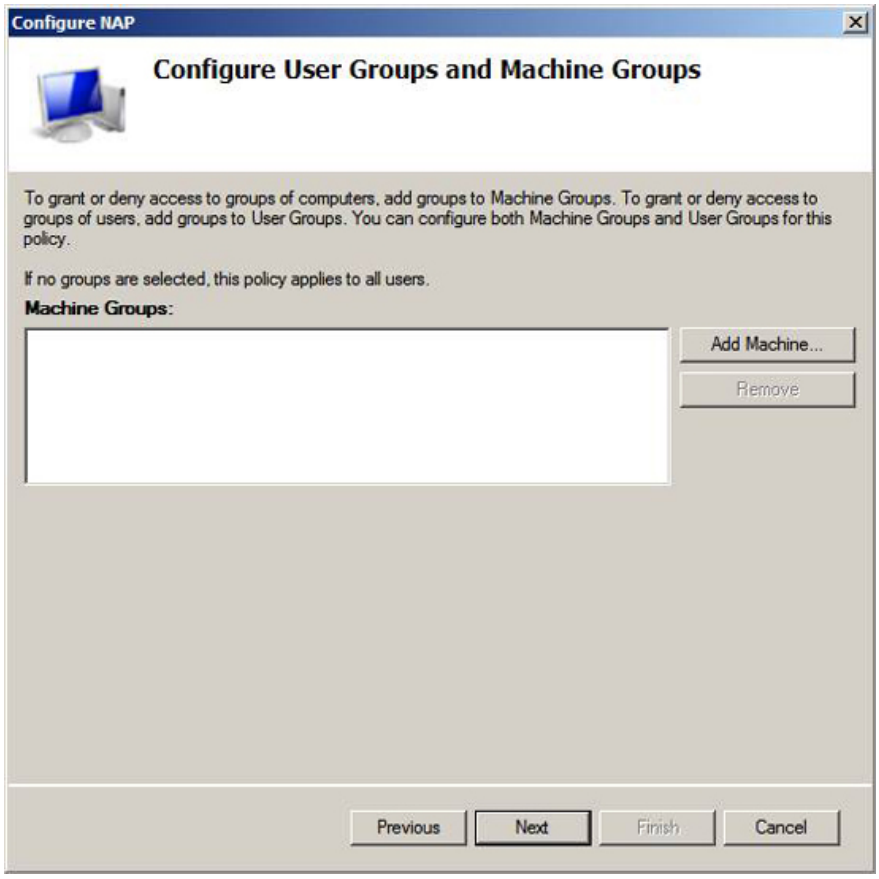

Figure 5

All computers need access to certain servers on the network. They need infrastructure servers such as Active Directory, DNS, DHCP and WINS servers. All computers need access to error-correction servers, which are computers that the computer does not meet the requirements for access to reach consensus.

On the **Specify a NAP Remediation Server Group page and URL page** , click the **Group** button to open the **New Remediation Server Group** dialog box. In the **New Remediation Server Group** dialog box **,** enter the group name in the **Group Name** text box. In this example, we name the group **Network Services** .

Click the **Add** button in the **New Remediation Server Group** dialog box. You will then see the **Add New Server** dialog box appear. In the **Add New Server** dialog box, enter the server name in the **Friendly name** box. In this example we enter a name for the domain controller, so we'll enter DC into this text box. The IP address of the domain controller is 10.0.0.2, so we will enter that address into the **IP address or DNS name** text box. If you know the name of the DNS server, you can enter that name in the text box and then click the **Resolve** button.

Click OK in the **Add New Server** dialog box **.**

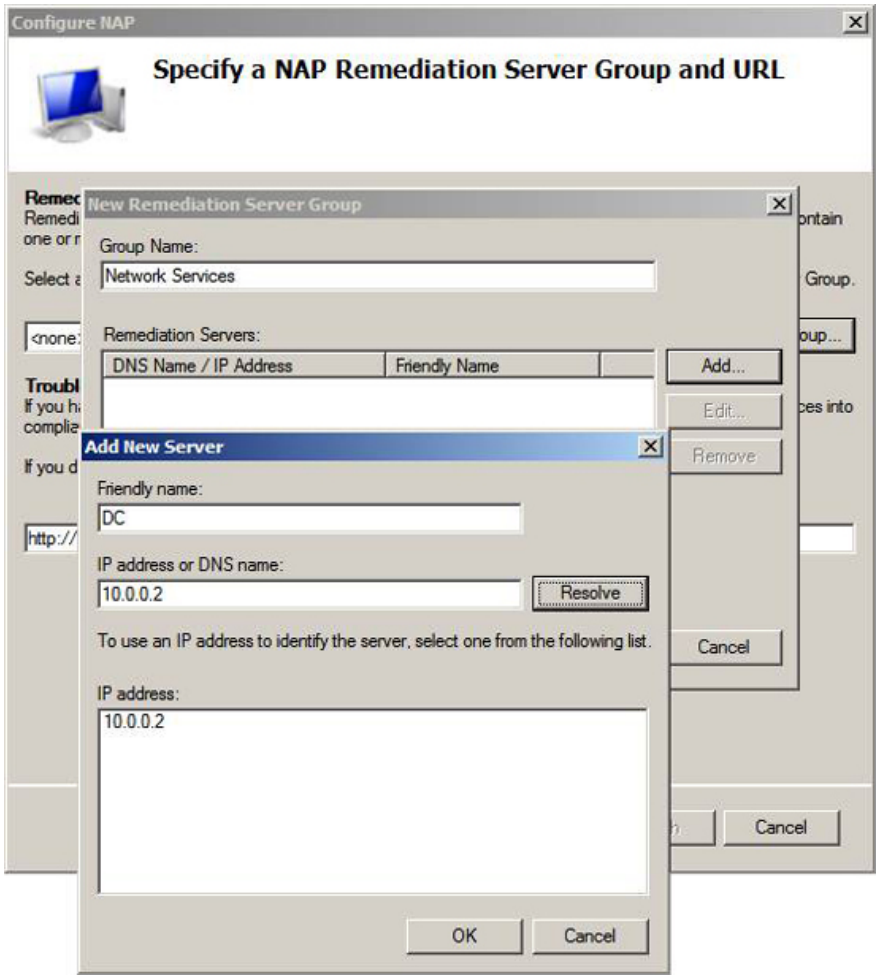

Figure 6

You should now see the name of the server group that fixes the error and the IP address of the server you added to the group. Remember, the purpose of this group is to remove it from the restrictions of NAP policy. The domain controller in this example is a computer that all domain members need to communicate with to log in. If you do not allow your NAP clients, whether they agree or not, to connect to the domain controller, they will not be able to log on to the network to become consensus after logging in.

Click **OK** in the **New Remediation Server Group** dialog box **.**

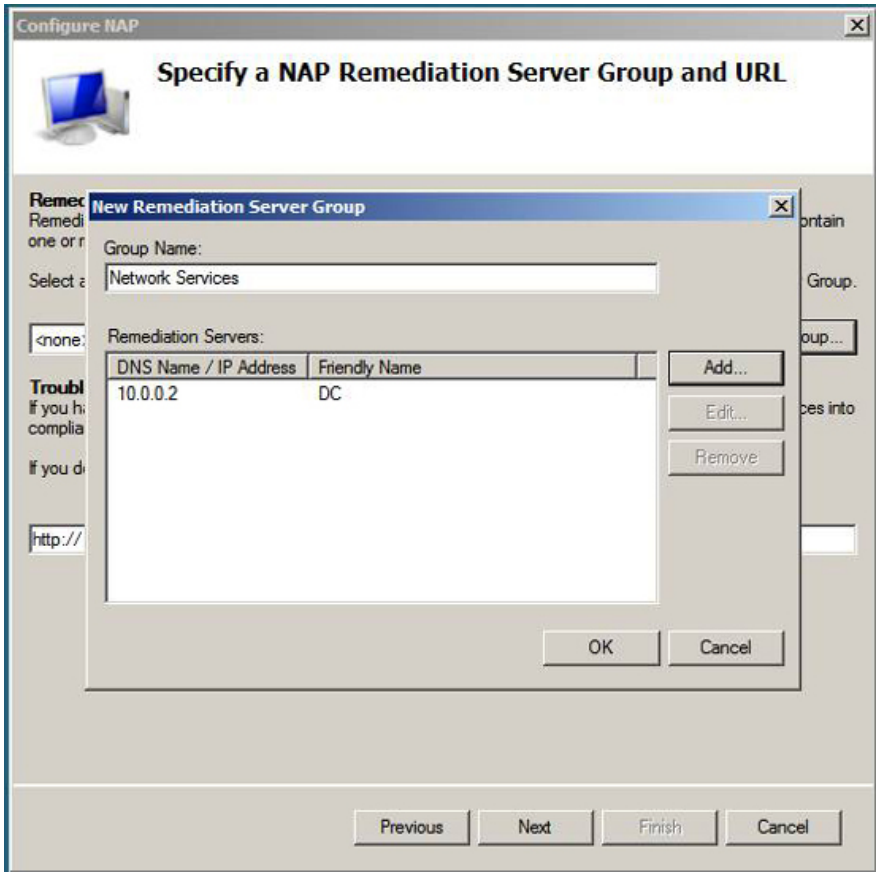

Figure 7

Click **Next** on the **Specify a NAP Remediation Server Group page and URL** . Note that we can also enter **Troubleshooting URL** on this page. We do not use any of this example, but sometimes you use it if you want to point users to a page that shows them how to become consensus after their computer is in a non-compliant state and cannot edit itself. error.

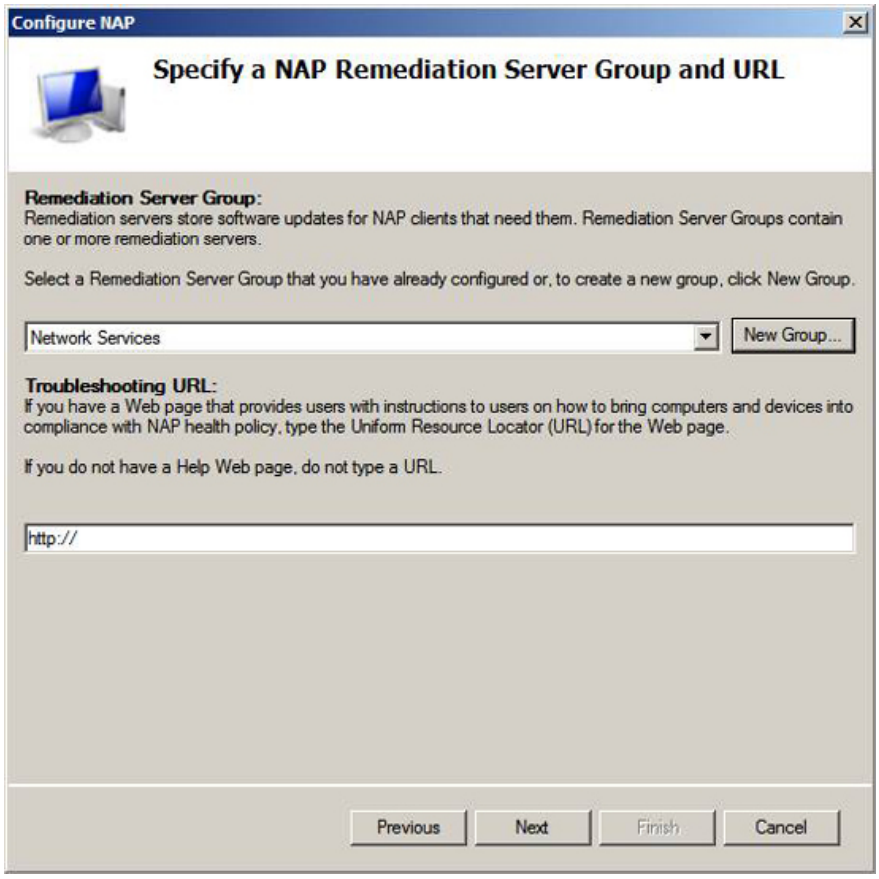

Figure 8

On the **Define NAP Health Policy page** , you can choose which System Health Validator you want to define a health policy for (Health Policy). By default, there is only one System Health Validator policy available in Windows Server 2008, which is the **Windows Security Health Validator** . Other software vendors may also group their System Health Validator products that you install into the NAP policy server.

Make sure there is a check mark in the **Windows Security Health Validator** checkbox. There is also a checkmark in the **Enable auto-remediation of client computers** check box. This option allows NAP client components to fix some problems on their own. For this example, if Windows Firewall is disabled, the NAP agent will activate Windows Firewall automatically.

In the **Access Network restrictions for the NAP-ineligible client computers** , you define what you want to do with non **-NAP-capable computers** . You have two options:

- ***Full network access to the NAP-ineligible client computers. Cho phép truy c?p ??n m?t m?ng ch? ?? b? t?t***
- *Reject all network access for unqualified NAP clients. Only allow restricted access to the network.*
- ***Allow full network access to NAP-ineligible client computers***
- *Allow access to unqualified NAP clients*

The first option is safer than the other option, while the second option is a more generous option. Your choice depends on the design goal for NAP. You can allow non-NAP-capable computers to access the network during the NAP deployment process and then, when the deployment process is complete, you will switch and execute

the NAP consensus machines.

Click **Next** on the **Define NAP Health Policy page** .

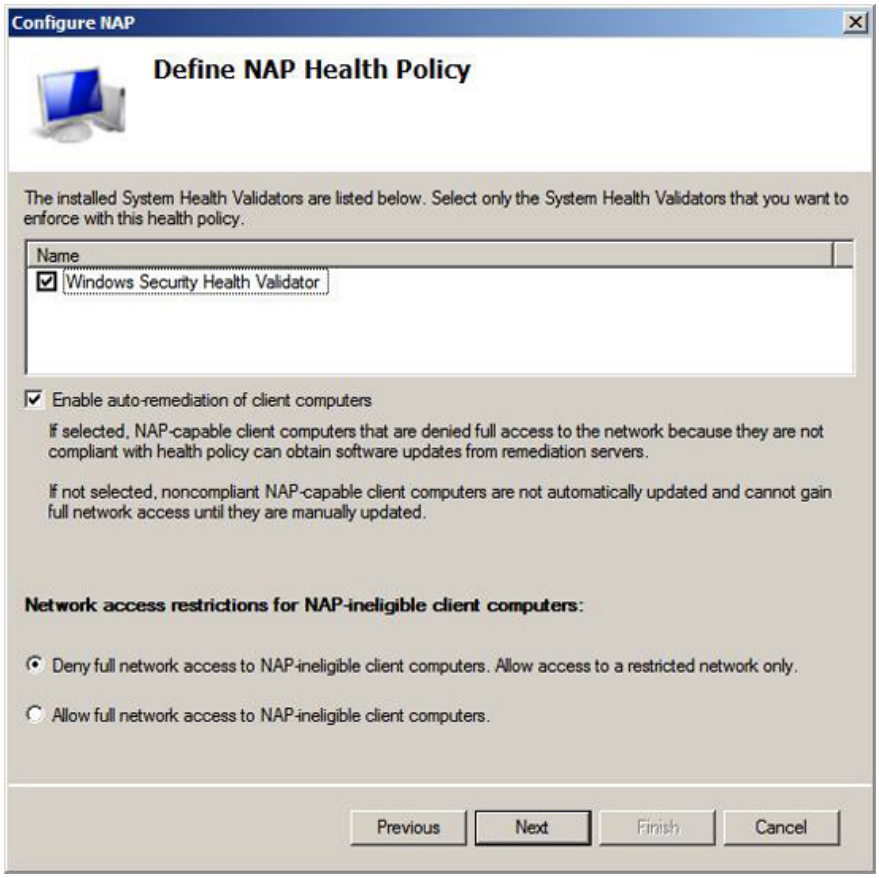

Figure 9

On **Completing NAP Enforcement Policy and RADIUS Client Configuration** pages, you can see **Health Policies** , **Connection Request Policies** , **Network Policies** and **Remediation Server Group** will be created by the wizard. We will take a closer look at these policies.

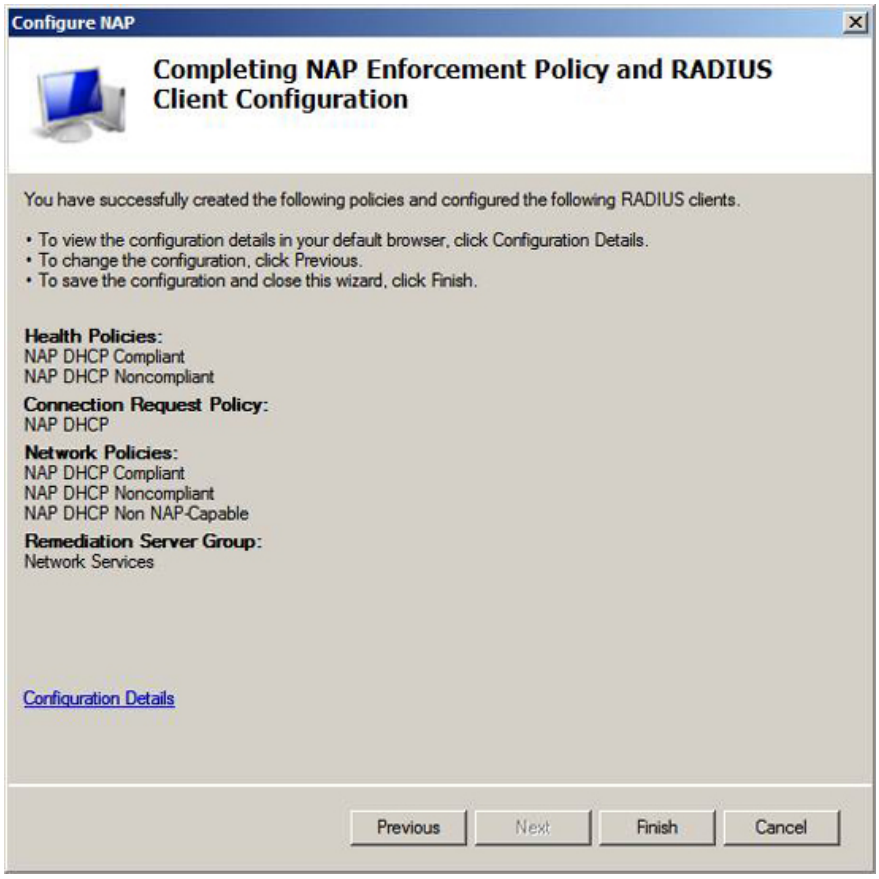

Figure 10

Note that there is only one **Configuration Details** link. When you click on this link, it will appear a page that provides detailed information about each policy that will be created by the wizard.

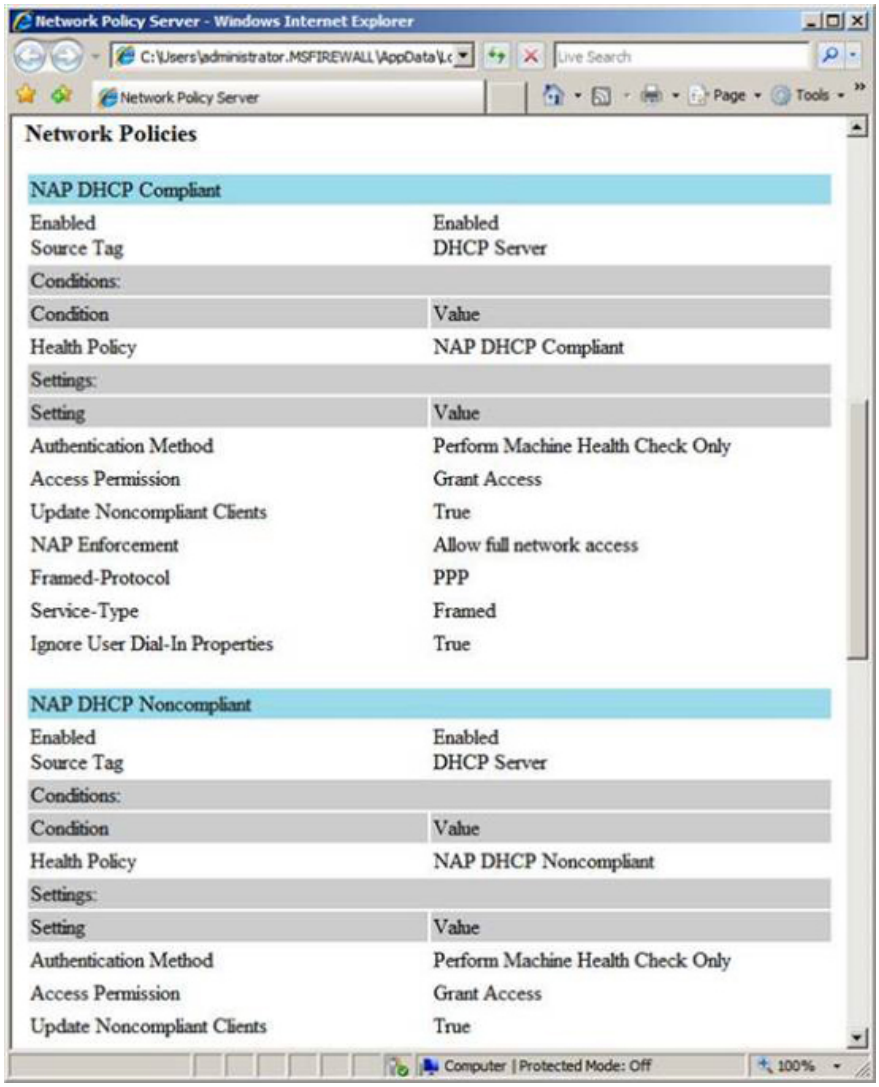

Figure 11

Conclude

In this part 2, I have discussed the NAP policy wizard and explained each option provided by this wizard. We have seen that the NAP policy wizard makes it much simpler to create a comprehensive NAP policy in the process of creating some Network, Health and Connection policies to control which computers can join the network. In the next part of this series, we will take a closer look at the rules and explanations of functions as well as the basic elements behind each of these rules.

You finished reading the article "**Use Group Policy Filtering to create a DHCP enforcement policy for NAP - Part 2**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com