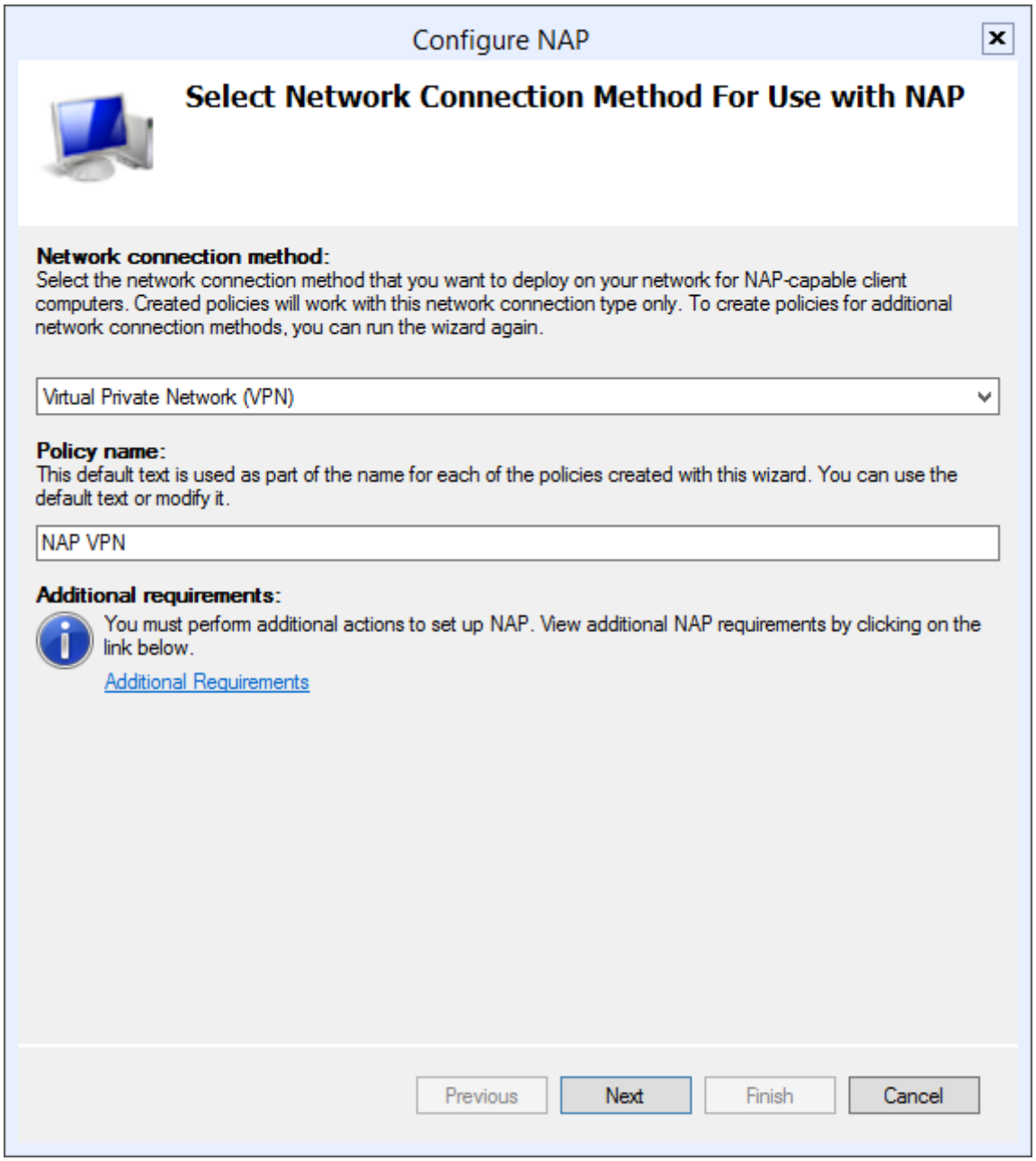
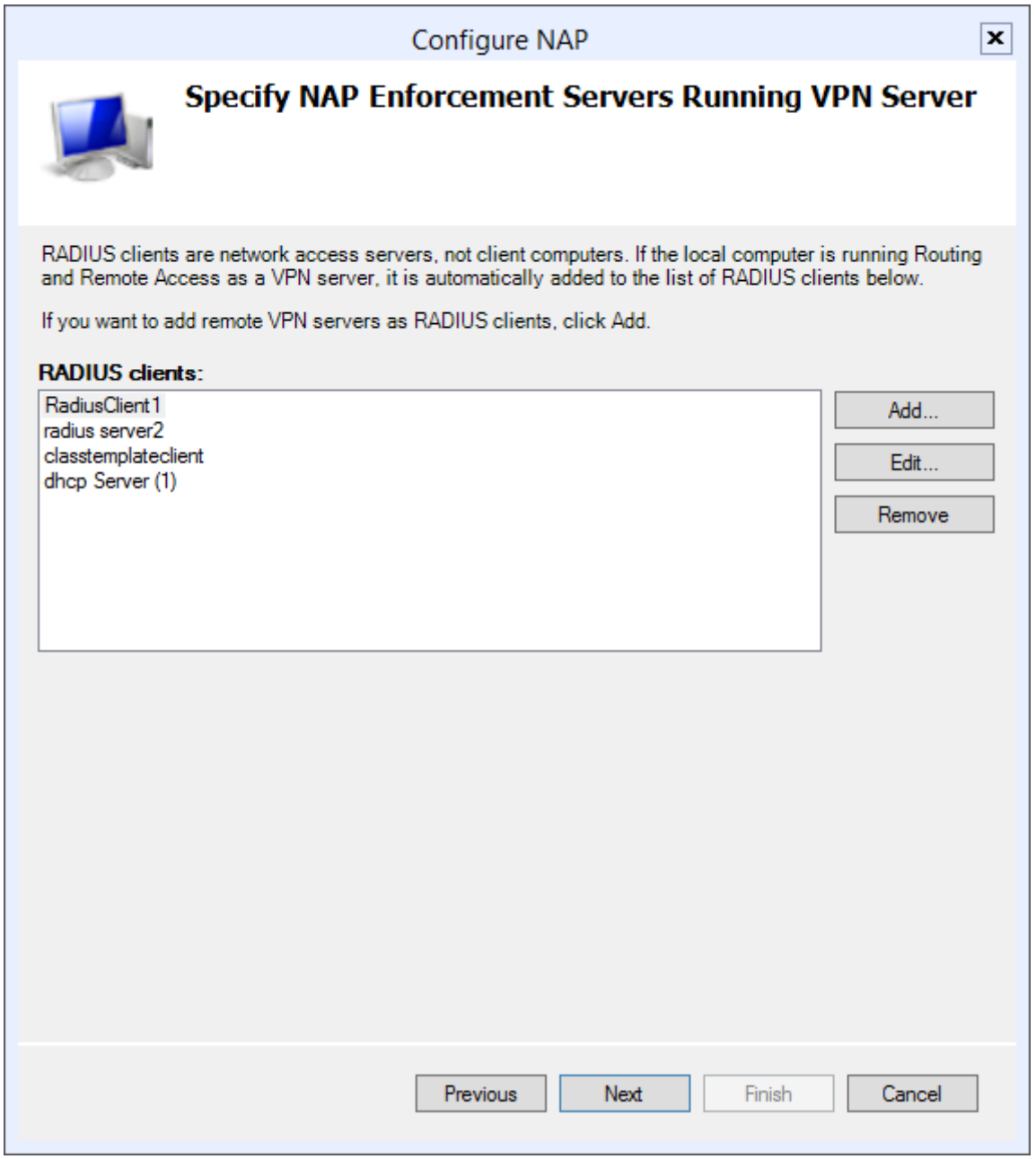
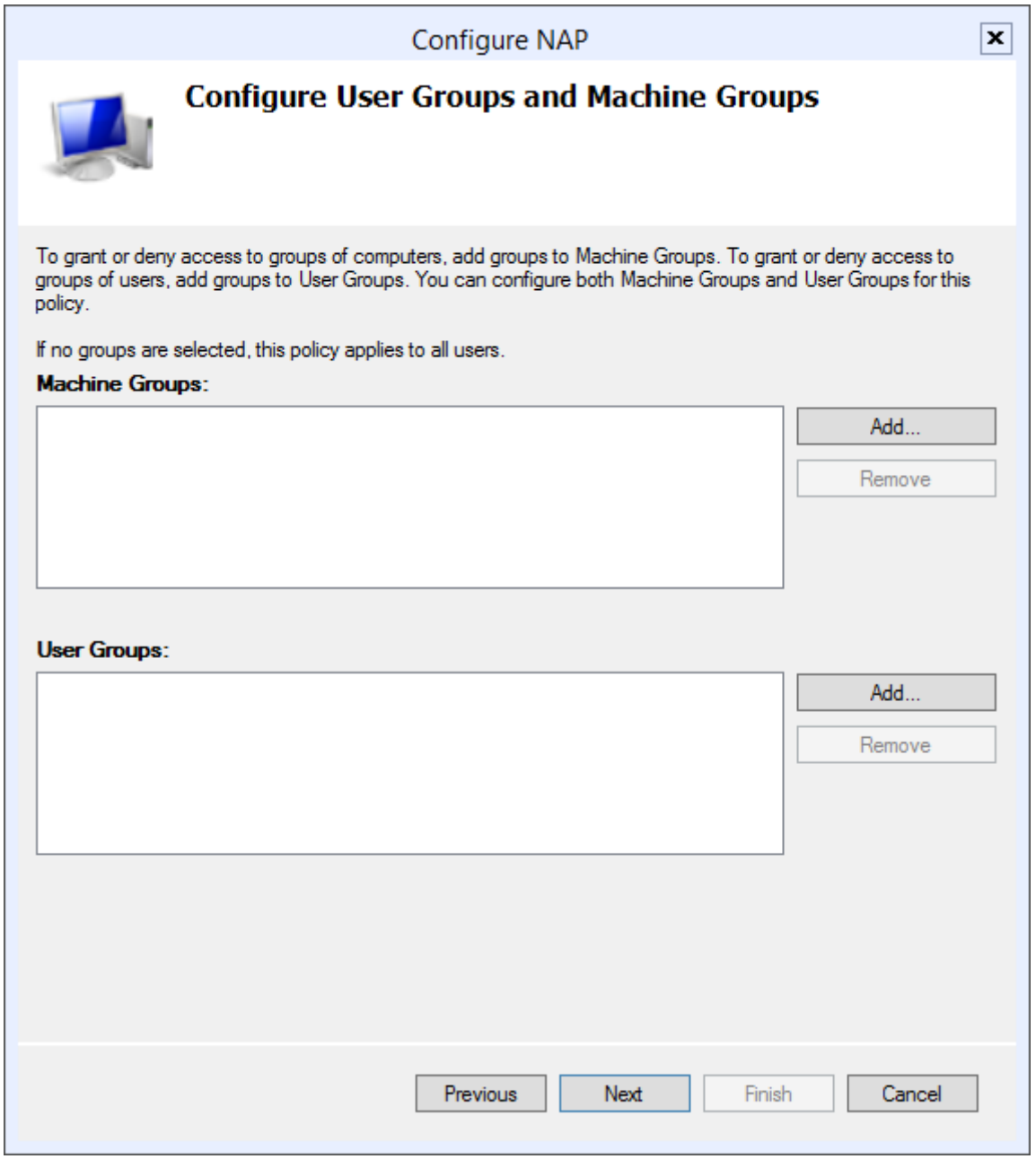
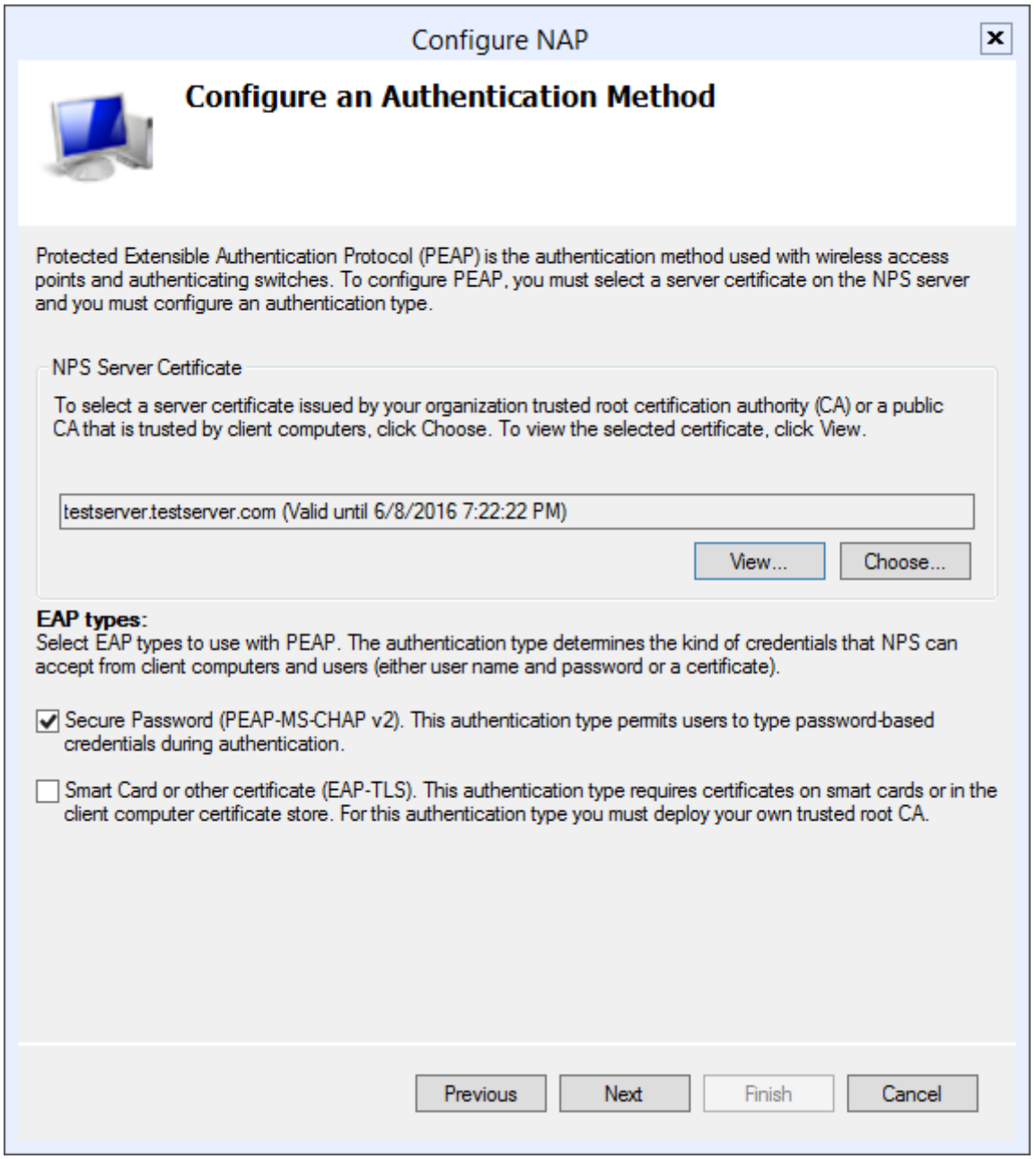
NAP VPN

SERVER 2012R2


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


Configure NAP
Specify NAP Enforcement Servers Running VPN Server
RADIUS clients are network access servers, not client computers. If the local computer is running Routing and Remote Access as a VPN server, it is automatically added to the list of RADIUS clients below.
If you want to add remote VPN servers as RADIUS clients, click Add.
RADIUS clients:
RadiusClient1
radius server2
classtemplateclient
dhcp Server (1)
Add...
Edit...
Remove
Previous
Next
Finish
Cancel


Configure NAP
Configure User Groups and Machine Groups
To grant or deny access to groups of computers, add groups to Machine Groups. To grant or deny access to groups of users, add groups to User Groups. You can configure both Machine Groups and User Groups for this policy.
If no groups are selected, this policy applies to all users.
Machine Groups:
Add...
Remove
User Groups:
Add...
Remove
Previous
Next
Finish
Cancel


Configure NAP
Configure an Authentication Method
Protected Extensible Authentication Protocol (PEAP) is the authentication method used with wireless access points and authenticating switches. To configure PEAP, you must select a server certificate on the NPS server and you must configure an authentication type.
NPS Server Certificate
To select a server certificate issued by your organization trusted root certification authority (CA) or a public CA that is trusted by client computers, click Choose. To view the selected certificate, click View.
testserver.testserver.com (Valid until 6/8/2016 7:22:22 PM)
View...
Choose...
EAP types:
Select EAP types to use with PEAP. The authentication type determines the kind of credentials that NPS can accept from client computers and users (either user name and password or a certificate).
Secure Password (PEAP-MS-CHAP v2). This authentication type permits users to type password-based credentials during authentication.
Smart Card or other certificate (EAP-TLS). This authentication type requires certificates on smart cards or in the client computer certificate store. For this authentication type you must deploy your own trusted root CA.
Previous
Next
Finish
Cancel

Configure NAP

Specify a NAP Remediation Server Group and 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.

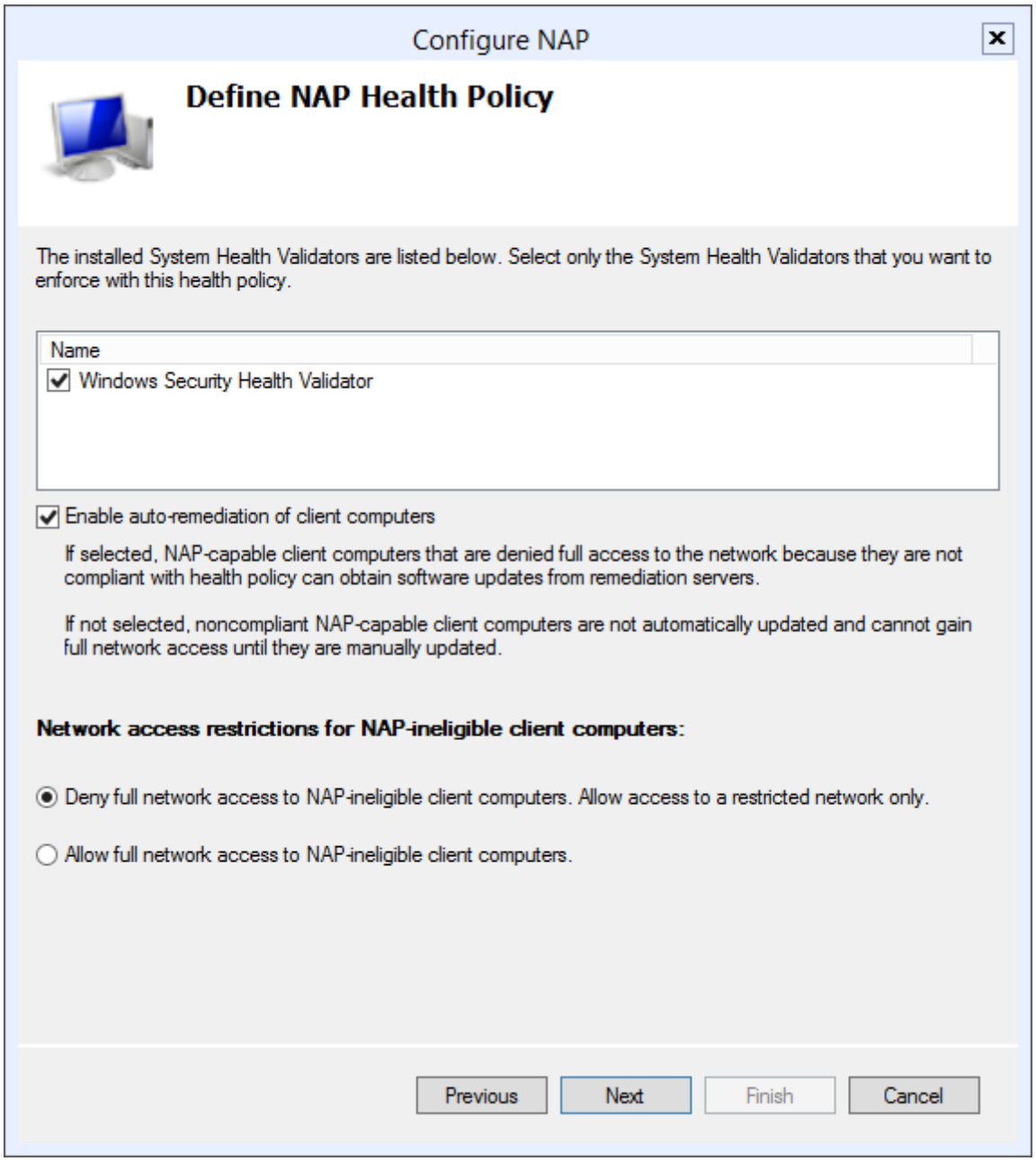
remediation group1 | New Group...

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.

http://

Previous | Next | Finish | 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
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

Configure NAP

Completing NAP Enforcement Policy and RADIUS Client Configuration

You have successfully created the following policies and configured the following RADIUS clients.

- To view the configuration details in your default browser, click Configuration Details.
- To change the configuration, click Previous.
- To save the configuration and close this wizard, click Finish.

Health Policies:
NAP VPN Compliant
NAP VPN Noncompliant

Connection Request Policy:
NAP VPN

Network Policies:
NAP VPN Compliant
NAP VPN Noncompliant
NAP VPN Non NAP-Capable

Remediation Server Group:
remediation group1

Configuration Details

Previous | Next | Finish | Cancel