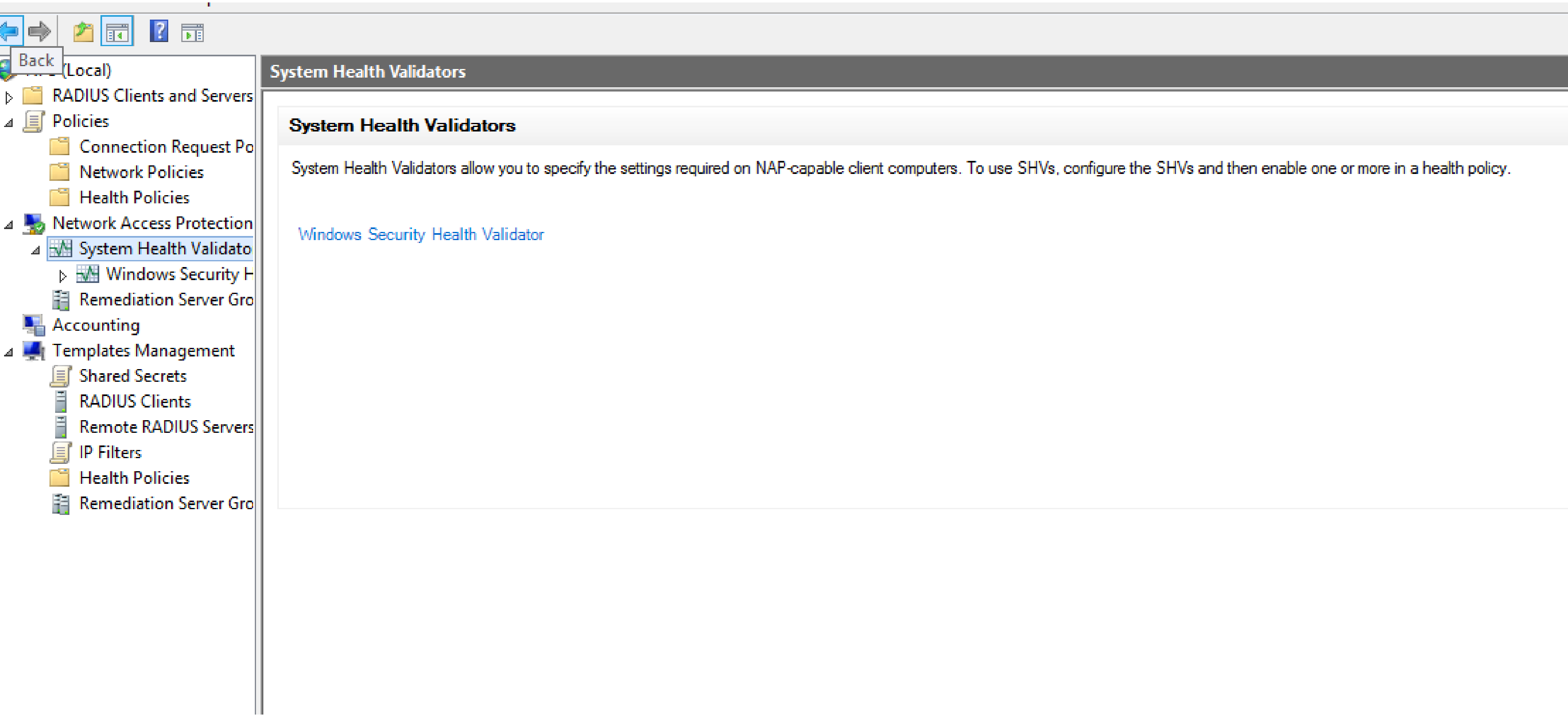
SYSTEM HEALTH VALIDATOR

When you install an SHV, it is added to the list of SHVs in the Network Policy Server (NPS) console and becomes available for use in health policies.

The Windows Security Health Validator (WSHV) is available by default.

Use the following procedure to configure the health requirements of an installed SHV.

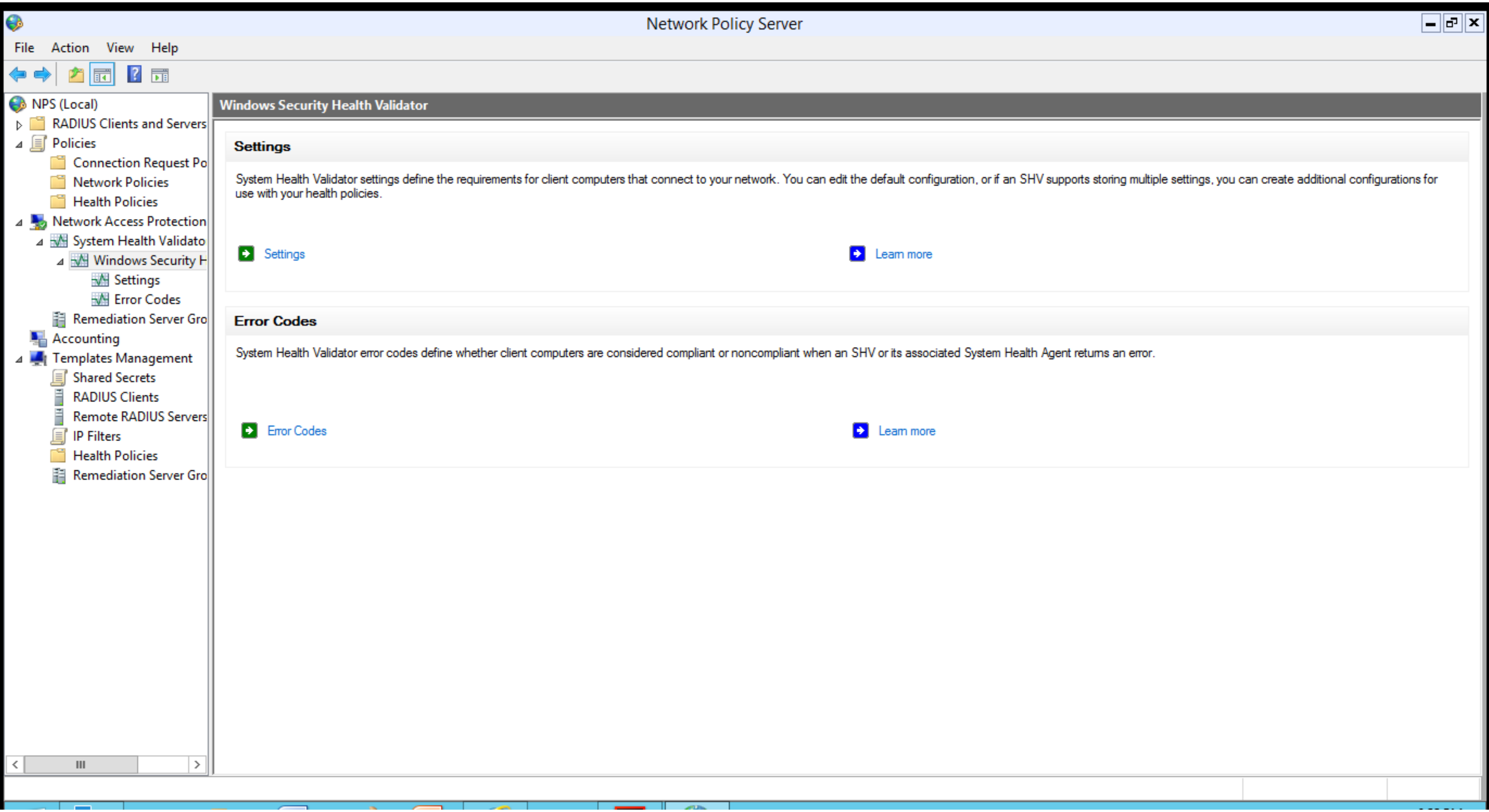
- In the NPS console tree, open **Network Access Protection**, and then click **System Health Validators**.
- In the details pane, under **Name**, double-click the name of the SHV you want to configure.
- To change the evaluation that is returned by NPS under specific error conditions, use the drop-down list next to each of the error conditions listed under **Error code resolution**. See the following example.



System Health Validators

System Health Validators allow you to specify the settings required on NAP-capable client computers. To use SHVs, configure the SHVs and then enable one or more in a health policy.

Windows Security Health Validator



Windows Security Health Validator

Settings

System Health Validator settings define the requirements for client computers that connect to your network. You can edit the default configuration, or if an SHV supports storing multiple settings, you can create additional configurations for use with your health policies.

Settings

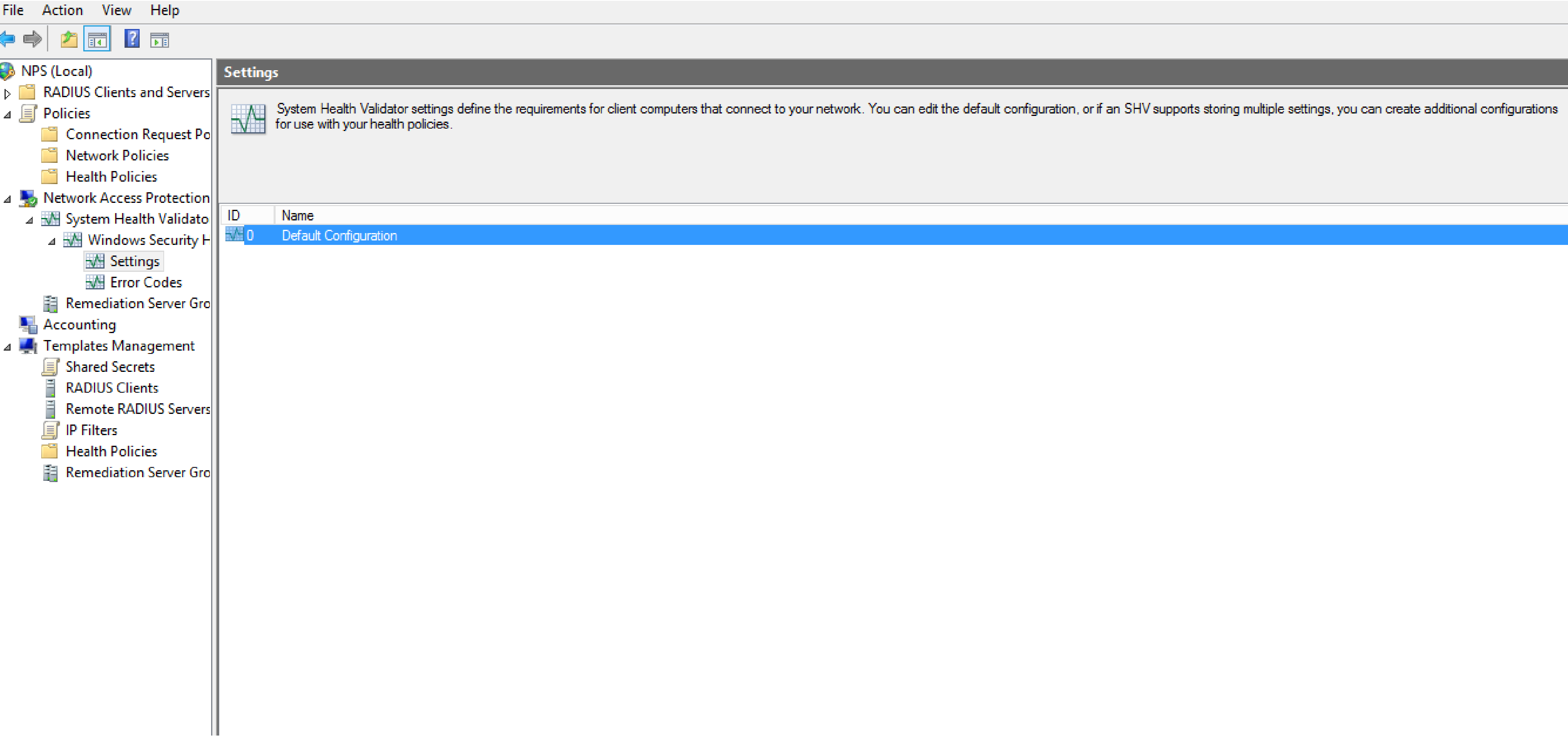
Learn more

Error Codes

System Health Validator error codes define whether client computers are considered compliant or noncompliant when an SHV or its associated System Health Agent returns an error.

Error Codes

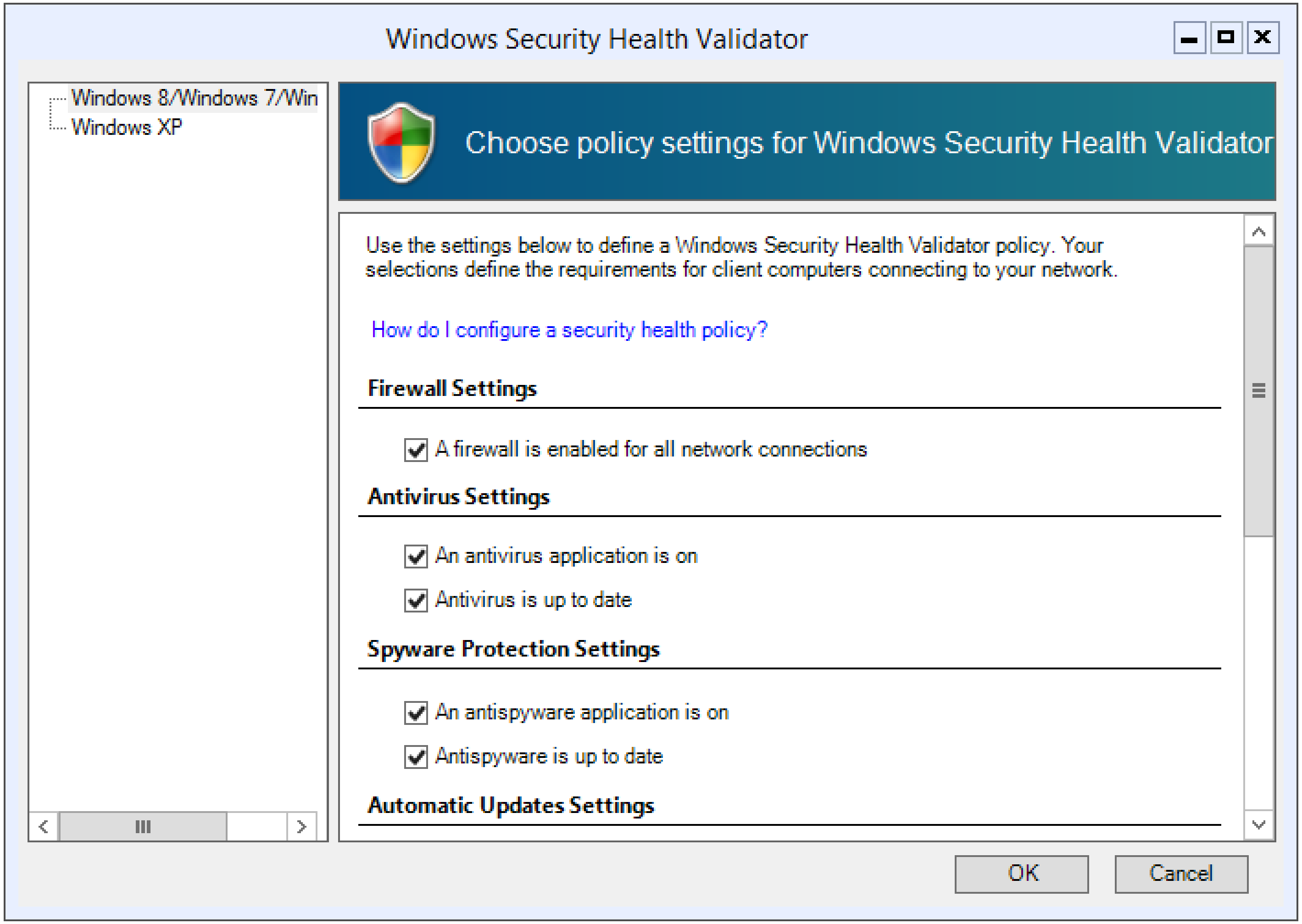
Learn more



Settings

System Health Validator settings define the requirements for client computers that connect to your network. You can edit the default configuration, or if an SHV supports storing multiple settings, you can create additional configurations for use with your health policies.

ID	Name
0	Default Configuration



Windows Security Health Validator

Choose policy settings for Windows Security Health Validator

Use the settings below to define a Windows Security Health Validator policy. Your selections define the requirements for client computers connecting to your network.

How do I configure a security health policy?

Firewall Settings

☑ A firewall is enabled for all network connections

Antivirus Settings

☑ An antivirus application is on

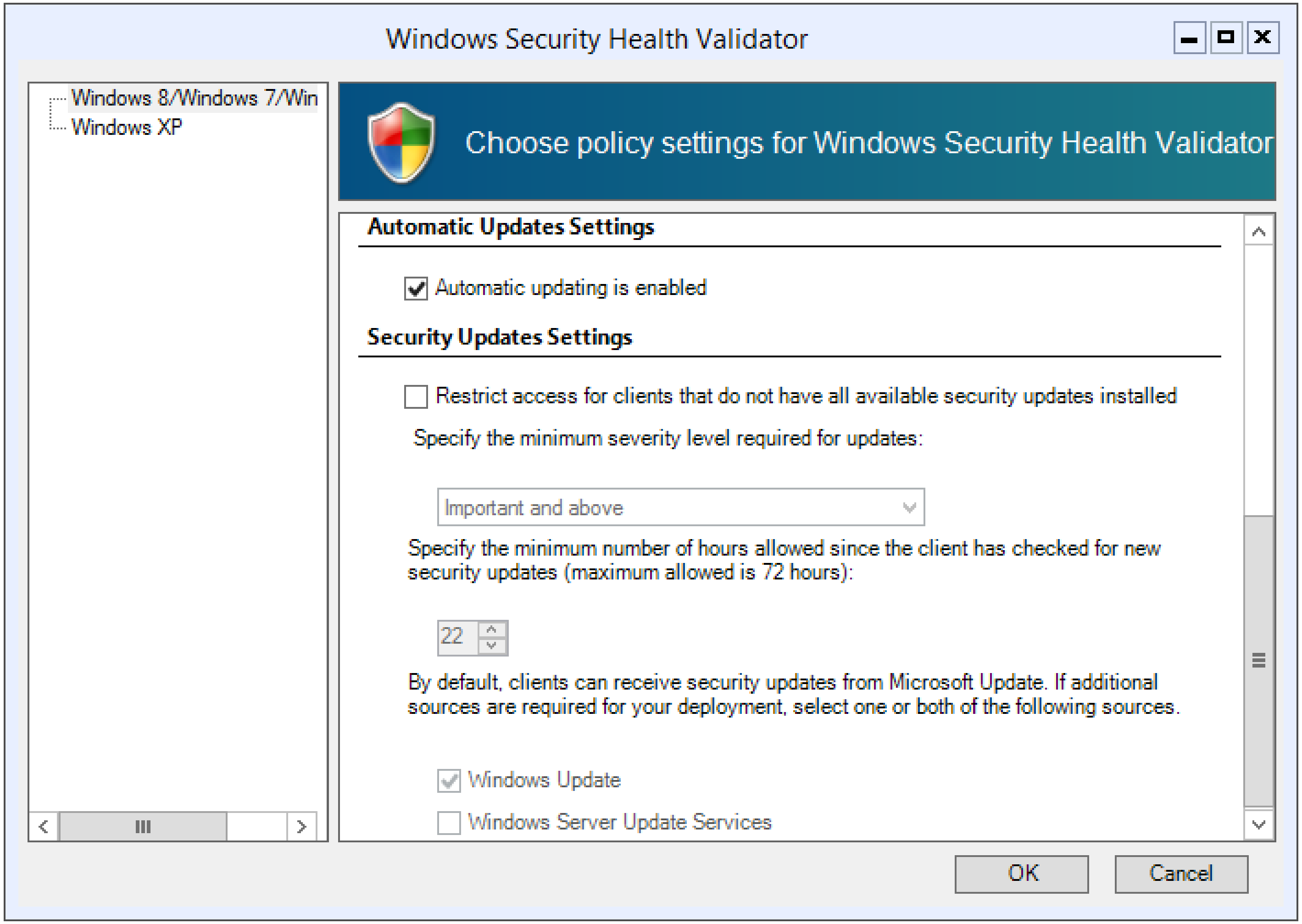
☑ Antivirus is up to date

Spyware Protection Settings

☑ An antispyware application is on

☑ Antispyware is up to date

Automatic Updates Settings



Windows Security Health Validator

Choose policy settings for Windows Security Health Validator

Automatic Updates Settings

☑ Automatic updating is enabled

Security Updates Settings

□ Restrict access for clients that do not have all available security updates installed

Specify the minimum severity level required for updates:

Important and above

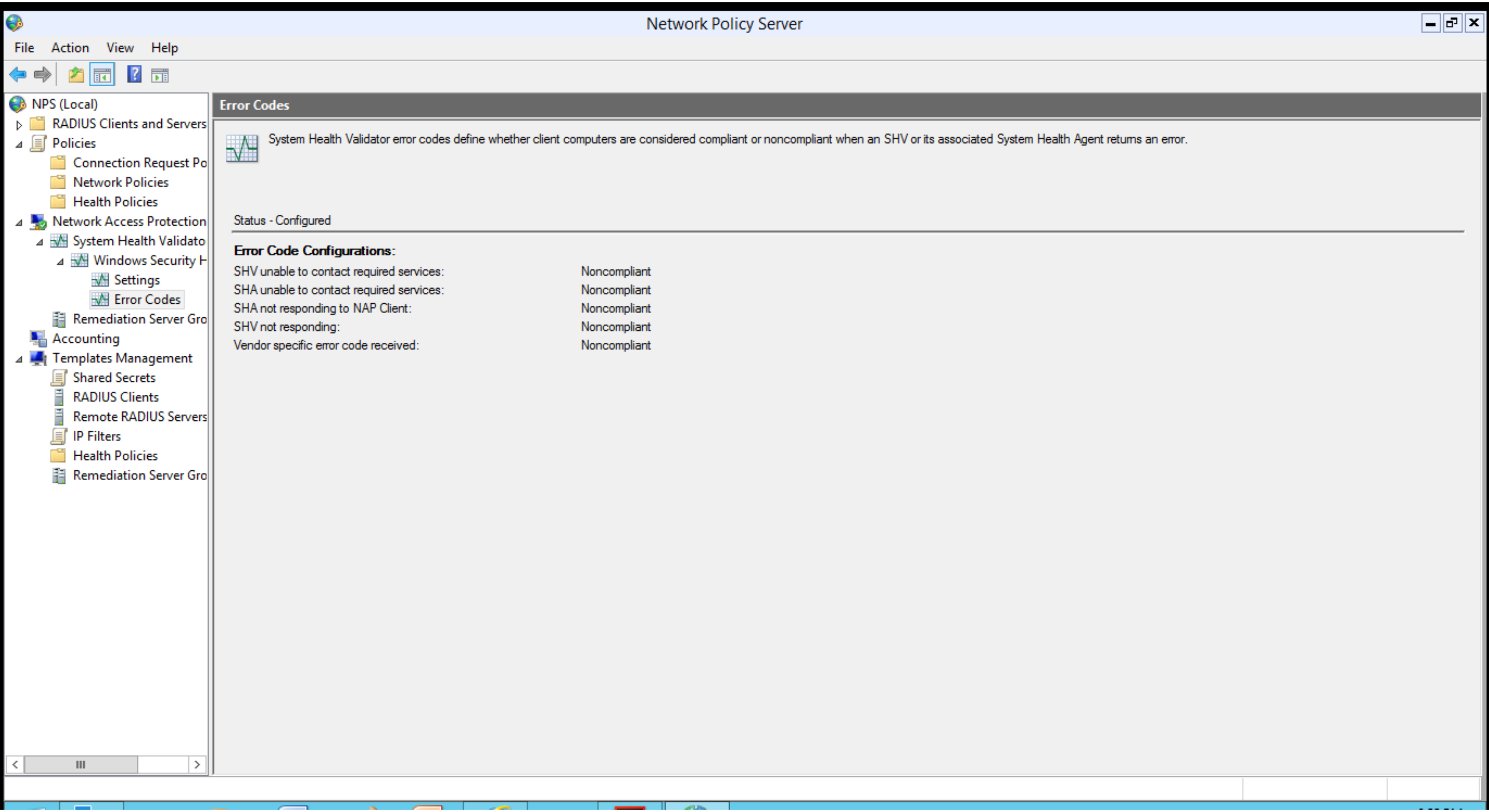
Specify the minimum number of hours allowed since the client has checked for new security updates (maximum allowed is 72 hours):

22

By default, clients can receive security updates from Microsoft Update. If additional sources are required for your deployment, select one or both of the following sources.

☑ Windows Update

□ Windows Server Update Services



Error Codes

System Health Validator error codes define whether client computers are considered compliant or noncompliant when an SHV or its associated System Health Agent returns an error.

Status - Configured

Error Code Configurations:

SHV unable to contact required services:	Noncompliant
SHA unable to contact required services:	Noncompliant
SHA not responding to NAP Client:	Noncompliant
SHV not responding:	Noncompliant
Vendor specific error code received:	Noncompliant