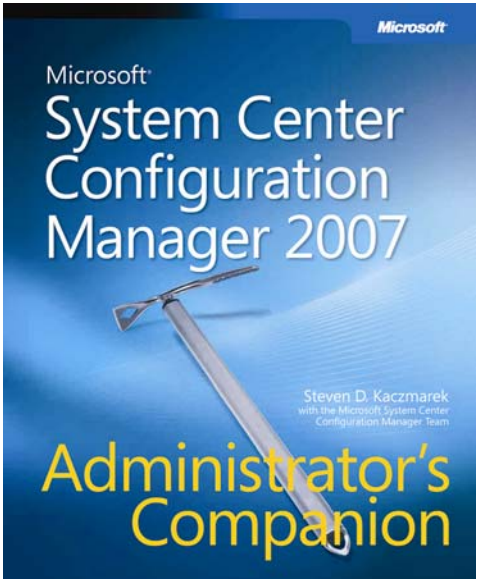


Microsoft® System Center Configuration Manager 2007 Administrator's Companion

Steven D. Kaczmarek with System Center Configuration Manager Team

To learn more about this book, visit Microsoft Learning at
http://www.microsoft.com/MSPress/books/9554.aspx

9780735623859

Microsoft Press

Table of Contents

Part III

Site Database Management

Chapter 15

Implementing Network Access Protection

Tomorrow's gatekeeper

Prevents dangerous talking!

NAP it to be safe.

~ Carol Bailey, Technical Writer, Configuration Manager

This chapter lifts the lid on Network Access Protection (NAP), one of the exciting improvements Microsoft includes with newer operating systems. It is another step closer to developing self-healing systems. Network Access Protection is a natural complement to System Center Configuration Manager in that it extends central management of software updates with compliance enforcement, and it can be used in concert with enforcing other components and applications on computers that you require for compliance.

In the long term, implementing Network Access Protection can help to protect your network assets. However, it should be considered one of many security strategies and does not replace other security tools or negate existing security practices. In addition, because of the potential for caching and inherent latency, Network Access Protection in Configuration Manager should not be considered a real-time security mitigation for noncompliant computers.

Understanding Network Access Protection

Most people think of Network Access Protection as a means of keeping noncompliant computers from accessing the network, where they could infect other computers with viruses. Network Access Protection can do this, but it is in fact far more sophisticated in its design and potential. This sophistication requires a learning curve for administrators,

a significant investment in the underlying infrastructure, and buy-in from management. Network Access Protection offers a tangible step toward the goal of self-healing systems, but its requirements, risks, and limitations must also be thoroughly understood before implementation if it is to fulfill the requirements of adding business value by decreasing the total cost of ownership.

So, before diving into how to configure Network Access Protection with Configuration Manager, take a step back and peel away some of the layers that make up the underlying Network Access Protection architecture. This will allow you to better understand how Configuration Manager fits into the Network Access Protection equation and also better understand the Network Access Protection configuration options in Configuration Manager.

The Many Layers of Network Access Protection

Network Access Protection uses the concept of "health" to define which elements and components should be configured or installed on computers. In the context of Configuration Manager, this relates to any software update that you can deploy through the software updates feature in Configuration Manager, including security updates, service packs, hardware vendor updates, and custom updates. In the context of the Windows Security Center, it could be basic Windows security checks such as whether the firewall is enabled, Windows Update is configured, and antivirus software is installed. As an open and extensible architecture, it allows other vendors to offer their own solutions that contribute toward the health of computers, such as a specific anti-spyware application that is installed and has the latest signature files.

For every health state that is checked in this way, you need a separate client component and a corresponding server component. On the client, a system health agent is responsible for assessing the health of a computer. On the server, a system health validator receives this information and validates it. These two components (system health agent and system health validator) are often abbreviated to just SHA and SHV. In Configuration Manager, the Configuration Manager System Health Agent is enabled when the Network Access Protection client agent is enabled, and the Configuration Manager System Health Validator is enabled when the System Health Validator point is installed.

Multiple system health agents on a single computer run under the direction of the Windows Network Access Protection agent. On computers running Windows Vista and Windows Server 2008, the Windows Network Access Protection agent is built into the operating system. For computers running Windows XP Professional with one of the latest service packs, you can install a Network Access Protection client that provides this functionality. One layer further down, each computer needs a Network Access Protection enforcement mechanism enabled that provides the networking layer that carries the packets related to Network Access Protection.

Network Access Protection enforcement mechanisms include DHCP, VPN, IPsec, 802.1X, and Terminal Services Gateway. You can use one or many enforcement mechanisms, depending on your business requirements. Each requires different setup and configuration, so it makes sense to choose selectively. For example, you might decide to configure DHCP enforcement only in a test lab as an initial proof of concept, with the view of configuring IPsec and 802.1X later on the production network. Or you might decide that Network Access Protection enforcement is required only for computers connecting over the VPN, but decide to test with DHCP first. Because Network Access Protection uses a layered architecture, the Network Access Protection processes of restricting network access and automatically remediating should be independent from the underlying Network Access Protection enforcement mechanisms. You can find step-by-step guides for the individual Network Access Protection enforcement mechanisms on the Network Access Protection Web site at *http://go.microsoft.com/fwlink/?LinkId=59125*.

The information that the system health agent sends to the system health validator is called the statement of health, which you will often see abbreviated to SoH. The system health validator validates this information and determines whether the client is compliant, noncompliant, or an error condition occurred that prevents the determination of the compliance status. The result of its validation is a statement of health response (SoHR). Statement of health responses from all system health validators are collected for a client so that a decision can be made about the client's network access. The decision is sent back to the client so that it knows whether it is deemed compliant or noncompliant and its resulting network access.

The Network Policy Server

The server that runs the system health validators and performs the role of a gatekeeper to the network is a computer running Windows Server 2008 that has installed on it the server role of Network Policy Server. It has policies configured that determine the network access that is allowed depending on whether the computer is compliant or noncompliant or whether an error condition occurred.

Although most people think of Network Access Protection as restricting network access for noncompliant computers, it can also give full network access but report the noncompliant status (known as reporting mode), and it can give full network access for a limited time (also known as deferred enforcement). This latter configuration provides a grace period until a set date that you configure. When this date is reached, a computer that remains noncompliant will have restricted network access.

Note This date is a set date for all computers and is not relative to the time that the client is found to be noncompliant. So you can't, for example, specify that all noncompliant computers have a week's grace to get compliant from the

time that they are found to be noncompliant. You can specify a date a week ahead, at which time all noncompliant computers will have restricted network access, even if they have been offline for six days.

For this configuration to work, you need a combination of policies configured on the Network Policy Server:

- **Connection request policy** This allows network access with at least one condition (such as the time and day condition, even if configured for 7 days and 24 hours) and can identify the type of Network Access Protection enforcement server you want to use.
- **Health policy** This identifies which system health validators are being used to determine the health of computers, and you will usually configure two health policies for each system health validator: one health policy in which health checks pass (indicating a compliant status) and another for when health checks fails (indicating a noncompliant status). After installing the system health validator point in Configuration Manager, you will be able to select the Configuration Manager System Health Validator in the Network Policy Server as one of the available system health validators when you configure health policies.
- **Network policy** This determines the network access that a computer will be given based on a number of factors that can include selected health policies—for example, giving a noncompliant computer restricted network access and a compliant computer full network access. Additionally, there is a separate option to invoke automatic remediation for noncompliant computers. However, Network Access Protection in Configuration Manager will always invoke remediation for noncompliant computers unless the reporting mode is selected. When the reporting mode is selected, Network Access Protection in Configuration Manager will never invoke remediation, even if the option to automatically update noncompliant computers is selected in the policy. In this scenario, use the standard software updates feature in Configuration Manager to install software updates on computers that require them.

When the Network Policy Server is being used with Network Access Protection, it is referred to as an NAP health policy server.

Real World The Balance of Power for Enforcing Compliance and Controlling Network Access

It is important to realize that it's the configuration of the policies on the Network Policy Server that ultimately determines whether noncompliant computers are remediated and whether they have full or restricted network access. Configuring

Network Access Protection in Configuration Manager does not provide this level of administrative control. Instead, the Configuration Manager administrator controls the definition of compliance with respect to software updates, which is then used by the health policies and network policies on the NAP health policy server. Of course, if you're the administrator for both Configuration Manager and the NAP health policy server, this division of control is not important. But if you have a different administrator for the NAP health policy server, plan a strategy for how you're going to work together and define the policies that collectively meet your business requirements.

Remediating Noncompliant Configuration Manager Clients

While it's undoubtedly satisfying to identify noncompliant computers and potentially prevent them from communicating with other computers on the main network, the key benefit in Network Access Protection is to automatically remediate them. After all, if the first priority for keeping them off the network is to ensure business continuity for existing network resources, the second priority should be to restore business continuity to the noncompliant computer quickly and without administrator or user intervention. Cue auto-remediation.

The means by which noncompliant Configuration Manager clients are remediated are exactly the same as when using the software updates feature in Configuration Manager. Clients still require access to their management point, software update point, and distribution points. These site systems are all considered potential remediation servers for Network Access Protection in Configuration Manager. The only difference during the remediation process for Configuration Manager is that software updates are installed with a high priority – before any software distribution packages or software updates that are not NAP–enabled. And, when remediation is complete, the client reassesses its health state and sends another statement of health.

If you are using IPsec as your Network Access Protection enforcement mechanism, configure software update points, distribution points, and management points as boundary servers. In Network Access Protection IPSec enforcement, boundary servers have the ability to communicate with both compliant and noncompliant Network Access Protection clients. Configuring these site system servers as boundary servers ensures that noncompliant Configuration Manager clients can access the remediation services they need. If you are using DHCP or VPN as your Network Access Protection enforcement mechanism, noncompliant Configuration Manager clients are given direct routes to the Configuration Manager remediation servers they need to access. There is no need to add these servers into a Remediation Servers Group on the Network Policy server, although you must add

infrastructure servers such as global catalog servers, DNS servers, and WINS servers into a Remediation Servers Group so that clients can complete the underlying server communications when required, such as management point location, name resolution, and authentication.

Planning for Network Access Protection in Configuration Manager

Now that you have a better understanding of the underlying processes involved when using Network Access Protection in Configuration Manager, you can move on to what needs to be in place before beginning to install and configure it.

Confirm the Windows Network Access Protection Infrastructure

At the time of this writing, Windows Server 2008 has not been released but has been working with Configuration Manager Network Access Protection since the beta 2 release of Windows Server 2008 (when it was still code named "Longhorn"). Configuration Manager Network Access Protection has been deployed in production on the Microsoft network with very successful results. For the latest information on how to deploy the Windows Network Access Protection infrastructure, refer to the Windows Network Access Protection Web site at *http://go.microsoft.com/fwlink/?LinkId=59125*.

The Windows Network Access Protection infrastructure needs to be in place and confirmed working before you attempt to add Configuration Manager into the equation. Use the step-by-step guides from the Windows Network Access Protection Web site to confirm a simple test using the default Windows Security Health Validator, such as checking that the firewall is enabled. This also requires that you have the correct operating system platforms on the client and server: either Windows Vista on the client, which has native Network Access Protection support, or the Network Access Protection Client for Windows XP; and Windows Server 2008 configured as an NAP health policy server.

Extend the Active Directory Schema

To use Network Access Protection in Configuration Manager, you must first extend the Active Directory schema for Configuration Manager 2007 and ensure that all sites that you want to enable for Network Access Protection are publishing to Active Directory Domain Services. This is the first feature in the history of the product that has required that the Active Directory schema is extended, and there are no workarounds. It is needed because when you mark a software update for Network Access Protection evaluation in

Configuration Manager, the site server writes a health state reference to Active Directory Domain Services, which is then retrieved by the System Health Validator point and used during the validation process. To store the health state reference, the Active Directory schema must be extended for Configuration Manager 2007, and the site must be published to Active Directory Domain Services.

Note The Active Directory attribute that Configuration Manager Network Access Protection uses is called smSSMSHealthState, which resides in the site's object in the System Management container. You can confirm that the site can support Network Access Protection by the presence of this attribute.

Additionally, the log file %systemdrive%\SMSSHV\SMS_SHV\Logs \SmsSHVADCacheClient.log on the System Health Validator point records "AD Schema is EXTENDED for SMSv4 Network Access Protection" when the System Health Validator point is installed and started.

Extending the Active Directory schema can be a big deal for many companies, so this needs careful planning and organizing beforehand. However, there is an additional factor here. You don't have to extend the site server's Active Directory forest but can extend and use another Active Directory forest to store and retrieve the health state reference. This involves additional configuration, but once set up, the behavior is the same, so it's worth considering whether extending the site server's Active Directory forest is problematic. You don't even need a trust relationship between the two forests, but if a trust doesn't exist, you will need to specify an account with credentials in the other forest.

Decide on Server Placement for the System Health Validator Points

With the ability to use another Active Directory forest to store and retrieve the health state reference comes another design consideration. You can place the System Health Validator points in a different Active Directory forest to the site server's forest. The System Health Validator point is one of the few site systems that are supported across forests, but note that they must still reside in an Active Directory domain. Although installation will still succeed on a workgroup computer, the System Health Validator point is not supported in this environment.

If you are installing the System Health Validator points in a different Active Directory forest to the rest of the Configuration Manager hierarchy, you must specify which Active Directory forest will store the health state reference. By default, the site server will write the health state reference to its own Active Directory forest, and the System Health Validator points will retrieve the health state reference from its own Active Directory forest. So you can see that if they don't use the same Active Directory forest, you must specify a

single Active Directory forest that will be used by both the site server and System Health Validator points. You'll come to the configuration part later of how to specify the Active Directory forest that will store the health state reference, but in the planning stages it's important to identify which Active Directory forest will be used and extend the schema for Configuration Manager if necessary.

Identify and Configure Firewalls

When you determine the design of where the System Health Validator points will be installed and which Active Directory forest will be used to store the health state references, check whether firewalls or other network perimeter devices are placed in between them and clients. This is particularly important if you are installing the System Health Validator points in a different Active Directory forest, because the forest represents a security boundary that is often protected by firewalls. If there will be intervening firewalls, identify which ports will need to be open to allow the traffic associated with Network Access Protection and ensure that these ports are open by the time you come to implement your solution. For a list of the ports you might need to configure, see the topic "Determine the Ports Required by Firewalls to Support Network Access Protection" in the Configuration Manager Documentation Library (*http://technet.microsoft.com/en-us/library/bb694170.aspx*).

Confirm Software Updates Operation

Enforcing compliance with software updates is an enhancement to and not a replacement for the standard software updates feature. Once hooked into the Windows Network Access Protection infrastructure, scanning and installing software updates uses the same processes as those used with the Configuration Manager software updates feature. If clients cannot successfully install software updates outside the Network Access Protection infrastructure, they will not be able to do so with Network Access Protection, with the potential consequence that they cannot access the network.

Note It pays to do thorough testing with the Configuration Manager software updates feature outside the Network Access Protection environment before implementing Network Access Protection!

Engage Other Business Groups

Network Access Protection is one of those features that crosses many administrative boundaries (and political ones!), and you will have to do your own homework here in determining who else needs to be involved when implementing Network Access Protection. For example, do you have a security team that advises which software updates are critical enough to risk a temporary loss of network connectivity for noncompliant com-

puters? Do you have service level agreements (SLAs) that might be affected by users having limited network access for a specified period of time that might influence how many software updates are selected for Network Access Protection in a single month?

And don't forget your help desk will need warning and training for how to deal with customer calls if noncompliant computers will have limited network access until remediation is successful. Help desk staff will require information on which software updates are included in Network Access Protection and the expected amount of time it takes for remediation to complete.

Additionally, plan whether you are going to make use of the in-house Network Access Protection troubleshooting Web site that users can be redirected to if remediation fails and they click the More Information button in the Network Access Protection dialog box. This could present users with useful data such as information about Network Access Protection and contact information for the help desk, links to download the software updates if remediation is failing, and other files that might be needed for compliance if automatic remediation fails. For more information about the troubleshooting Web site, see the Network Access Protection product information or the topic "Configuring the Remediation User Experience for Configuration Manager Network Access Protection" in the Configuration Manager Documentation Library (*http://technet.microsoft.com/en-us/library/bb680466.aspx*).

Educate Your Users

The process of educating users about changes to computer management might be handled by the help desk, but it's important enough to call it out separately here. Particularly if you are going to implement Network Access Protection with limited network access for noncompliant computers, you must warn and educate users in advance. Explain to users the business benefits in protecting the network from noncompliant computers and then provide them with appropriate information about what they should do if they find themselves with limited network access.

The information provided to users will vary from company to company and depend on how tech savvy the users are. In an ideal environment, provide users with the details of the software updates that will be included in Network Access Protection and the date the updates will be enforced so that users can proactively install them. In a nonurgent scenario, use software update deployments with a deadline that is at least a few days ahead of when those updates will be included with Network Access Protection and encourage users to install the software updates or risk having limited network access.

On the other hand, if you operate with minimum user interaction, the advice might be to wait a specified period of time before calling the help desk if users experience problems accessing resources and see the Network Access Protection icon in the notification area.

Decide on the user experience and processes that will be used ahead of time and make sure that the help desk is included in these decisions.

Identify Users and Computers That Need Exemptions

When you create a software update deployment in Configuration Manager, you identify which computers will receive the software update through collection targeting. However, Network Access Protection in Configuration Manager doesn't use collection targeting. A software update marked for Network Access Protection will automatically be targeted to computers assigned to the site, and this configuration flows down the hierarchy with the following consequences:

- If a Configuration Manager client is installed but not yet assigned to a site, the Configuration Manager client will not evaluate the software update for Network Access Protection compliance because at this point it does not know whether the Configuration Manager Network Access Protection client agent should be enabled or disabled. In this scenario, the client sends a special statement of health to the System Health Validator point to indicate that it hasn't yet received its client policy. The System Health Validator point gives the client a compliant health status so that it can find its assigned site and download its client policy.
- If the Network Access Protection client agent is not enabled and the computer is capable of supporting Network Access Protection (it is NAP-capable), the Configuration Manager client will not evaluate the software update for Network Access Protection compliance. However, it will still send a statement of health, and the System Health Validator point gives the client a compliant health status.
- If the Network Access Protection client agent is enabled, but the computer is not capable of supporting Network Access Protection, perhaps because it is running Windows XP Service Pack 1 (it is NAP-ineligible), the Configuration Manager client will not evaluate the software update for Network Access Protection compliance. In this scenario, no statement of health can be sent, and network policies on the NAP health policy server determine whether these computers have full network access or limited network access. However, Network Access Protection remediation is not possible.
- If the Network Access Protection client agent is enabled and the computer can support Network Access Protection (for example, it is running Windows Vista), the software update will be automatically evaluated for Network Access Protection compliance. The only way to exclude Configuration Manager clients from evaluating software updates marked for Network Access Protection is to disable the Configuration Manager Network Access Protection client agent, or ensure that they are not running an operating system capable of supporting Network Access Protection,

or disable the Windows Network Access Protection Agent service on an NAP-capable computer.

Instead of relying on these exceptions, use policy exemptions when configuring the network policies on the NAP health policy server. This is particularly important if you have computers that do not have the Configuration Manager client installed. In this scenario, an NAP-capable computer will still send a statement of health, but it will not contain any information from the Configuration Manager System Health Agent. If the NAP health policy server is expecting a compliant or noncompliant health state for Configuration Manager, this scenario will result in an error condition. By default, error conditions are mapped to noncompliant. If noncompliant computers are configured for limited network access, this computer will have limited network access and report an error message of "SHA Not Present" with unsuccessful remediation. Automatic remediation is not possible in this scenario because remediation in Configuration Manager is restricted to software updates. Configuration Manager Network Access Protection cannot automatically install the Configuration Manager if there is a problem with the client installation or the client is not installed.

If you have computers that do not have the Configuration Manager client installed, and should have in order to manage them, you can use this process to enforce the installation of the Configuration Manager client. However, you will have to make sure that users (or help desk engineers) can manually install the Configuration Manager client when the computer has restricted network access. This can be achieved, for example, if you are using the troubleshooting Web site and configure a link to install the client. For optimal user experience, ensure that the installation is as streamlined as possible to keep to a minimum the delay in getting the computer back onto the full network. This is particularly important if you are using VPN Network Access Protection enforcement and users have to download the client source files over a slow, remote network.

However, in many cases there will be genuine reasons why a computer should not have the Configuration Manager client installed. These computers must be identified and included in an exemption policy that does not expect compliance information from the Configuration Manager System Health Validator.

You might need other exemption policies for computers that do have the Configuration Manager client installed but should be treated differently. For example, even if they are noncompliant, they should have unlimited network access or full network access for a limited time. Another possibility is to create exemption policies that do not restrict network access outside the hours that the help desk is open.

Identify these exemptions ahead of time, agree to them with stakeholders, and document them so that this information can be shared with the help desk and the NAP health policy server administrator. And don't forget to test that they work as expected before you go live on a production network!

For more information about configuring exemption policies for Network Access Protection, see the Network Access Protection product documentation.

Checkpoints for Identifying Which Clients Can Support Network Access Protection

The Network Access Protection client status in Configuration Manager is one of the following: NAP-capable (the client can support Network Access Protection, either natively or after installing the Network Access Protection client); NAP-upgradable (the client doesn't natively support Network Access Protection but could be upgraded to support Network Access Protection with the Network Access Protection client); or NAP-ineligible (the client cannot support Network Access Protection).

Note You can use the Network Access Protection report "List of NAP-capable and NAP-upgradable computers" to identify the NAP-capable and NAP-upgradable computers, and use the following SQL query to identify how many NAP-capable clients you have: *Select NapEnabledCount from v_Network Access ProtectionSystemInfo.*

Implementing Network Access Protection in Configuration Manager

When you've completed your planning for Network Access Protection, you're ready to start implementing and configuring Network Access Protection in Configuration Manager.

Important More than for any other feature in Configuration Manager, make sure that you plan for Network Access Protection before you begin implementing it. When other features are misconfigured or lack a planning step, they most likely result in an error or no action. However, when Network Access Protection is misconfigured or lacks a planning step, it could result in a massive denial of service with all computers on the network having indefinite restricted network access.

Creating and Configuring the System Health Validator Point

The decision process involved with installing the System Health Validator point is slightly different from installing other site system roles in Configuration Manager. First, it must be installed on a computer running Windows Server 2008 that has the role of Network Policy Server installed on it. Second, there is no direct correlation between Configuration Manager clients in a site and a System Health Validator point. Network Access

Protection clients are directed to the System Health Validator point through the Windows Network Access Protection infrastructure, not through the Configuration Manager infrastructure.

Generally, the decision as to where and how many System Health Validator points to install is not the Configuration Manager administrator's choice, but the Windows Network Access Protection administrator's decision. Wherever a Network Policy Server is installed and configured for Network Access Protection, you should install a Configuration Manager System Health Validator point. This might be a single server or multiple servers. It might mean that all System Health Validator points reside in one Configuration Manager site—not necessarily the central site in the hierarchy—or that they are installed in multiple Configuration Manager sites. The Configuration Manager site does not have to be enabled for Network Access Protection in order to install a System Health Validator point.

When you have multiple System Health Validator points, bear in mind that they share a common configuration within a site. If, for some reason, you need different settings for System Health Validator points, your only choice is to install them in different sites. However, wherever possible, use the same configuration for all System Health Validator points in the hierarchy to ease administration and troubleshooting. When all System Health Validator points share a common configuration, the behavior of clients using them will be consistent, which is especially important when NAP-capable clients roam between Configuration Manager sites.

Installing a System Health Validator Point

The process for installing a System Health Validator point is no different from installing any other site system role. Remember, however, that it must be installed on a computer running Windows Server 2008 that is configured with the server role of Network Policy Server. Configuration Manager will not prevent you from installing it if these requirements are not met, but the installation will not be successful.

To create a site system on the computer that is configured for an NAP health policy server and install the Configuration Manager System Health Validator point, follow these steps:

1. In the Configuration Manager Administrator Console, expand the site's Site Settings node and then right-click Site Systems.
2. Click New and choose Server from the context menu to launch the New Site System Server Wizard.
3. In the General page of the wizard, provide the following information:
   - **Name:** Type the short name of the NAP health policy server.

- **Specify A Fully Qualified Domain Name (FQDN) For This Site Server On The Intranet:** Type the FQDN of the NAP health policy server.
- **Specify An Internet-Based Fully Qualified Domain Name For This Site System:** Leave this field blank. The System Health Validator point is not supported with Internet-based client management.
- **Use The Site Server's Computer Account To Install This Site System:** Leave this selected if the site server's computer account can be authenticated on the computer running Windows Server 2008.
- **Use Another Account For Installing This Site System:** Select this option only if you are installing the System Health Validator point in a different Active Directory forest, and there is no trust relationship that will allow the site server's computer account to be authenticated on the computer running Windows Server 2008. Then click Set, and in the Windows User Account dialog box, specify a user account and credentials that have local administrator permissions on the computer running Windows Server 2008.
- **Enable This Site System As A Protected Site System:** Do not select this option. It is not applicable for a System Health Validator point.
- **Allow Only Site Server Initiated Data Transfers From This Site System:** Do not select this option. It is not supported for a System Health Validator point.

4. Click Next to display the System Role Selection page in the wizard.
5. Select System Health Validator Point and then click Next to display the System Health Validator page.
6. Read the information relating to the System Health Validator point, which includes the following points:
   - Remember that this site system role must be installed on a computer running Windows Server 2008 and configured for Network Access Protection policies.
   - The System Health Validator point configuration is on the System Health Validator Point Component Properties page.
   - If you are configuring the System Health Validator point in a different Active Directory forest, you might have additional configuration for the storage and retrieval of the health state reference.
7. Configuring the System Health Validator points is covered in the next section, so click Next.
8. On the Summary page of the wizard, click Next, and if you are happy with your configuration, click Next, and then click Close.

9. In the results pane, you should now see the additional site system, with the roles displayed as ConfigMgr Component Server, ConfigMgr Site System, ConfigMgr System Health Validator Point.

10. If you have additional System Health Validator points to install, repeat steps 1 through 9.

Configuring the System Health Validator Points

For most installations, you will not need to change the default settings for the System Health Validator points. However, if you have installed a System Health Validator point in a different Active Directory forest, or if you want to store and retrieve the health state references from a different Active Directory forest, additional configuration is required.

To configure System Health Validator points, follow these steps:

1. In the Configuration Manager Administrator Console, expand the site's Site Settings node and click Component Configuration. In the results pane, double-click System Health Validator Point Component.

   You will see that the System Health Validator Point Component Properties dialog box has two tabs, the General tab and the Health State Reference tab, as shown in Figure 15-1.

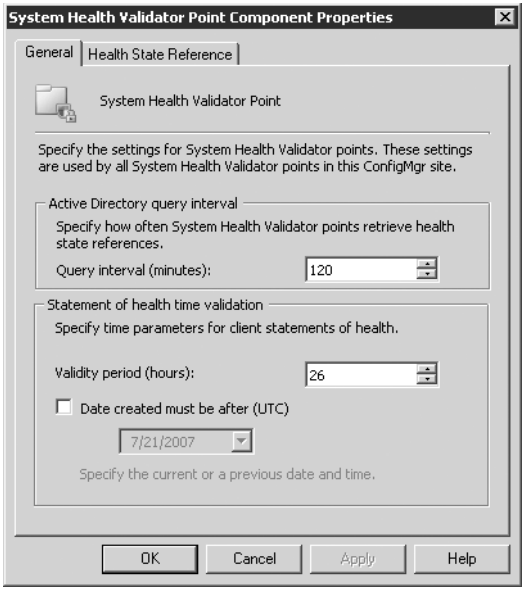


Figure 15-1 The General tab of the System Health Validator Point Component Properties dialog box

2. In the General tab, the Query Interval is how often the System Health Validator points retrieve the health state reference from Active Directory Domain Services. The default is every 2 hours from startup of the System Health Validator service. If this value is set too high, the compliance of clients might be based on out-of-date information, which could result in clients that haven't downloaded their latest Configuration Manager client policy having full network access when they should not. However, if this value is set too low, it can result in clients being found noncompliant, not because they need software updates, but because their compliance assessment is out of date. A recommended value is twice the value specified for the policy polling interval in the Computer client agent properties (by default, set once an hour). Change the Query Interval (Minutes) value if the default of 120 minutes is not suitable for your environment.

3. Also on the General tab is the Validity Period (Hours). The default value is every 26 hours. A computer will cache its statement of health and can present this to the System Health Validator point to increase performance. Not using a cached statement of health will delay connecting to the network and incur additional processing on the client. This setting configures how old the cached statement of health can be before the System Health Validator point considers it out of date. If the cached statement of health is older than the configured validity date, the client will be considered noncompliant. In this scenario, remediation is invoked for the client to reevaluate its compliance and produce a new statement of health. A recommended value is to ensure that this setting is higher than the Network Access Protection evaluation schedule, which is configured on the Network Access Protection client agent properties (and by default, configured for once every 24 hours). Change the Validity Period (Hours) value if the default of 26 hours is not suitable for your environment.

4. Finally on the General tab is the Date Created Must Be After (UTC) option. Do not use this setting as a day-to-day configuration. It is designed specifically for a zero-day exploit scenario, where you have just configured a software update for Network Access Protection and it is imperative that clients immediately include this software update in their Network Access Protection compliance assessment rather than wait for them to next download their client policy. In the situation where you have just deployed the critical software update, you would then select this option and set the current date and time. Any client presenting a statement of health that was not as current as this value would be deemed noncompliant. Remediation in this scenario involves the client downloading the latest Configuration Manager Network Access Protection policies, reevaluating Network Access Protection compliance, and resending a current statement of health. Configure this option only if you have just configured a Network Access Protection policy for an urgent evaluation.

5. The Health State Reference tab, as shown in Figure 15-2, is where you specify whether you want to use a different Active Directory forest, and if so, the additional configuration that this requires.

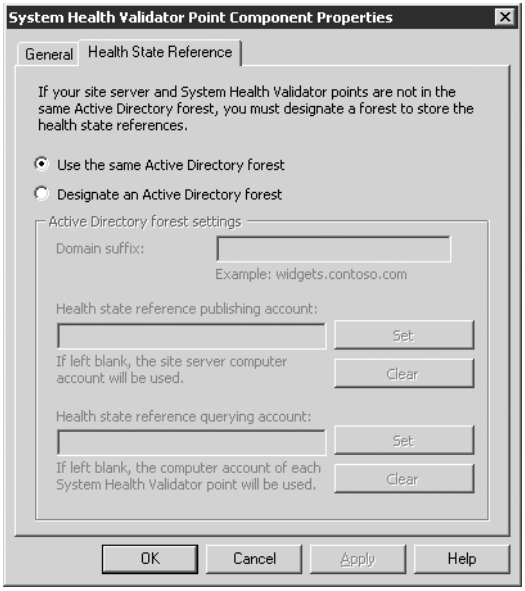


Figure 15-2 The Health State Reference tab of the System Health Validator Point Component Properties dialog box

6. If you are using just one Active Directory forest, there is nothing to configure on this tab. Keep the default selection of Use The Same Active Directory Forest.

7. If you are using a different Active Directory forest, select the Designate An Active Directory Forest option and then specify the domain suffix in the Domain Suffix field.

8. If there is a trust relationship between the site server and the designed Active Directory forest such that the site server's computer account can be authenticated, there is no need to specify the Health State Reference Publishing Account. Where this is not the case, click Set and specify in the Windows User Account dialog box a user account and credentials that will be authenticated in the designed Active Directory forest. Then click OK.

9. If there is a trust relationship between the System Health Validator point site system servers and the designed Active Directory forest such that the site system servers' computer account can be authenticated, there is no need to specify the Health State Reference Querying Account. Where this is not the case, click Set and specify in the Windows User Account dialog box a user account and credentials that will be authenticated in the designed Active Directory forest. Then click OK.

10. Click OK to close the System Health Validator Point Component Properties dialog box. Any new System Health Validator points added to the site will be automatically configured with these settings.

Enabling and Configuring Network Access Protection Client Settings

You will need to enable the Network Access Protection client agent, because this client agent is not enabled by default on new sites or sites that have been upgraded from SMS 2003. Additionally, you might want to change the default client agent settings, which include how often the client evaluates its Network Access Protection compliance and whether a fresh scan will be forced for each evaluation.

Checkpoints for Enabling Network Access Protection in Configuration Manager

Before you enable Network Access Protection in Configuration Manager, make sure that the Windows Network Access Protection Agent service is running—and set to start automatically—and that the Network Access Protection enforcement client is enabled. In addition to starting these manually, Group Policy can be used to configure these on both Windows Vista and Windows XP with the Network Access Protection client installed. See the Windows Network Access Protection documentation for more information about configuring these underlying components.

If the Windows Network Access Protection service is not started before enabling the Configuration Manager Network Access Protection client agent, the computer will behave as if it is NAP-ineligible and will not send a statement of health. Network policies on the NAP health policy server determine whether NAP-ineligible computers have full network access or limited network access, and Network Access Protection remediation is not possible.

If the Windows Network Access Protection service is mistakenly not started before enabling the Configuration Manager Network Access Protection client agent, start the service and then restart the Configuration Manager client. Alternatively, if restarting all clients is not practical, disable the Configuration Manager Network Access Protection client agent, wait a full policy cycle (by default, set to 60 minutes), and then enable it again.

Additionally, if you are deploying an operating system in a Network Access Protection environment by using the operating system deployment feature in Configuration Manager, make sure that either the reference computer is fully configured for Windows Network Access Protection before installing the Configuration Manager client, or that additional steps are added to the task sequence, which includes a restart before installing the Configuration Manager client.

More Info See the topic "Planning for Operating System Deployment in a Network Access Protection-Enabled Environment" at *http://technet.microsoft.com/en-us/library/bb892794.aspx* in the Configuration Manager Documentation library for more information.

To enable the Network Access Protection Client Agent and configure Network Access Protection client settings, follow these steps:

1. In the Configuration Manager Administrator Console, expand the site's Site Settings node and click Client Agents. In the results pane, double-click Network Access Protection Client Agent.
2. The General tab has the single setting Enable Network Access Protection On Clients, as shown in Figure 15-3. Select this option.

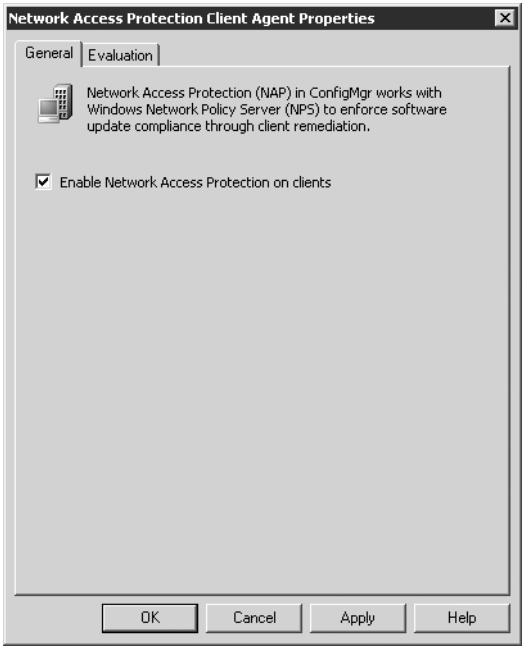


Figure 15-3 The General Tab of the Network Access Protection Client Agent Properties dialog box

3. On the Evaluation tab, the configuration options relate to how often and when a client evaluates its Network Access Protection compliance for Configuration Manager. This tab is shown in Figure 15-4.

4. By default, the Network Access Protection evaluation schedule is in universal coordinated time rather than local time. If you want a client to evaluate compliance using local time, clear the UTC (Coordinated Universal Time) check box.
5. By default, the Force A Fresh Scan For Each Evaluation check box is not selected. This allows the client to use a cached statement of health to speed up connectivity times and reduce processing usage on the client. If you are particularly security conscious and want to ensure that a new statement of health is produced every time, select this option. This option can mean a few minutes wait without full network access while the client reevaluates compliance and produces a new statement of health.

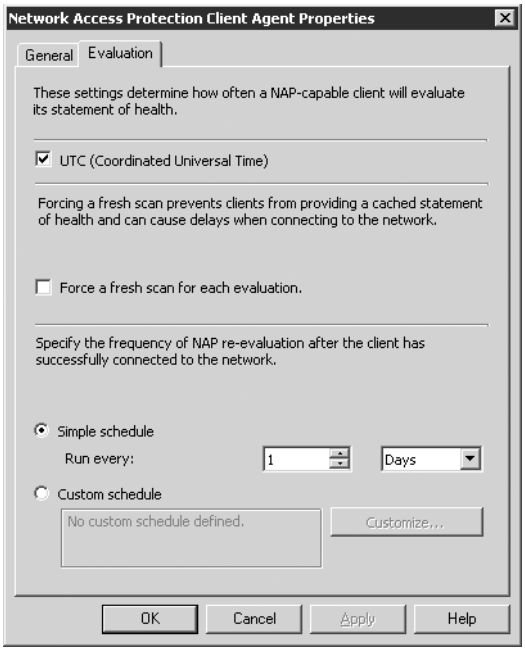


Figure 15-4 The Evaluation tab of the Network Access Protection Client Agent Properties dialog box

6. By default, Network Access Protection evaluation occurs once a day, using the Simple Schedule. As with any schedule in Configuration Manager, you can change this by using the Simple Schedule drop-down boxes or select the Custom Schedule option, click Customize, and configure your choice of schedule.

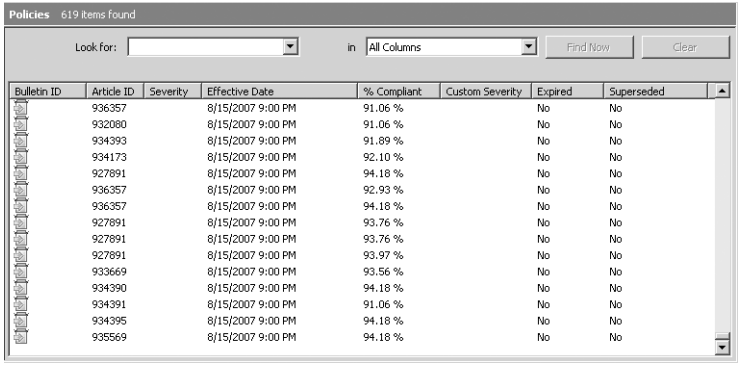
These settings affect all clients assigned to the site that are capable of supporting Network Access Protection. If the client cannot support Network Access Protection, the settings are ignored.

Note Even if the Network Access Protection client agent is disabled, clients that are capable of supporting Network Access Protection will still send a statement of health. However, the statement of health contains information that tells the System Health Validator point that the client agent is disabled, which results in the System Health Validator point giving the client a compliant health state.

Creating and Managing Network Access Protection Policies

After enabling the Network Access Protection client agent, you can select software updates for Network Access Protection evaluation. Click the Network Access Protection node in the Configuration Manager console and then press F5 to refresh the display. A new child node called Policies appears under Network Access Protection.

Click the Policies node, and the results pane shows columns that are shared with the software updates feature—all except one unique column called Effective Date. The Effective Date is when the software update will be included in Network Access Protection evaluation. Until that date, the software update that is selected for Network Access Protection lies dormant, which gives users a chance to install the software update themselves and provides adequate time for the software update package to replicate to all distribution points. Figure 15-5 shows sample Network Access Protection policies with their effective date configured for August 15, 2007, together with their current compliance status.



Bulletin ID	Article ID	Severity	Effective Date	% Compliant	Custom Severity	Expired	Superseded
	936357		8/15/2007 9:00 PM	91.06 %		No	No
	932080		8/15/2007 9:00 PM	91.06 %		No	No
	934393		8/15/2007 9:00 PM	91.89 %		No	No
	934173		8/15/2007 9:00 PM	92.10 %		No	No
	927891		8/15/2007 9:00 PM	94.18 %		No	No
	936357		8/15/2007 9:00 PM	92.93 %		No	No
	936357		8/15/2007 9:00 PM	94.18 %		No	No
	927891		8/15/2007 9:00 PM	93.76 %		No	No
	927891		8/15/2007 9:00 PM	93.76 %		No	No
	927891		8/15/2007 9:00 PM	93.97 %		No	No
	933669		8/15/2007 9:00 PM	93.56 %		No	No
	934390		8/15/2007 9:00 PM	94.18 %		No	No
	934391		8/15/2007 9:00 PM	91.06 %		No	No
	934395		8/15/2007 9:00 PM	94.18 %		No	No
	935569		8/15/2007 9:00 PM	94.18 %		No	No

Figure 15-5 Sample Network Access Protection Policies displayed in the Policies home page

When you select a software update to be included in Network Access Protection evaluation, it appears as a Network Access Protection policy, as shown in Figure 15-5, that you can easily monitor and edit from this Policies node. Each Network Access Protection policy results in writing to the health state reference in Active Directory Domain Services so that the System Health Validator point knows that a change was made to Configuration

Manager Network Access Protection policies. Although each software update selected for Network Access Protection evaluation is displayed as a separate Network Access Protection policy, in reality all Network Access Protection policies for the site are stored in a single Network Access Protection policy for the site. It is this single Network Access Protection policy that creates the health state reference in Active Directory Domain Services.

There are actually a number of ways to select software updates for Network Access Protection evaluation, but one of the easiest is to use the New Policies Wizard from the Policies node. To create Network Access Protection policies using the New Policies Wizard, follow these steps:

1. In the Configuration Manager Administrator Console, right-click the Policies node and then select New Policies to launch the New Policies Wizard.
2. In the Select Software Updates for Network Access Protection page of the wizard, a list of software updates that have been downloaded and are stored as software update packages in Configuration Manager are displayed. See Figure 15-6 for an example. If the software update you want to include in Network Access Protection evaluation is not displayed, it is most likely not downloaded, and you will have to download it using standard software update operation (for example, using the Download Updates Wizard). If this is not the first time you have run the New Policies Wizard, another explanation for a missing software update is that it has already been selected for Network Access Protection evaluation.

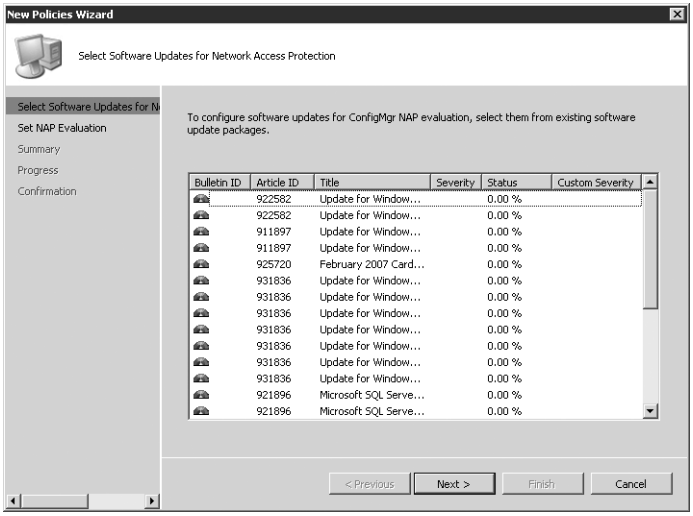


Figure 15-6 The Select Software Updates for Network Access Protection page of the New Policies Wizard where you select the software updates to include in Network Access Protection evaluation

3. Select one or more software updates displayed and click Next.
4. On the Set NAP Evaluation page of the wizard, as shown in Figure 15-7, specify the date when you want the software update to be included in Network Access Protection evaluation by the client. Select either the As Soon As Possible option (appropriate for an urgent update, such as a zero-day exploit) or select the Date And Time option to specify the exact date and time.

> **Note** If you specify As Soon As Possible and the software update package has not yet replicated to all distribution points, a noncompliant client might have to request the software update over slow WAN links because it is not yet locally available. This can result in network saturation, long remediation times, and even timeout errors.

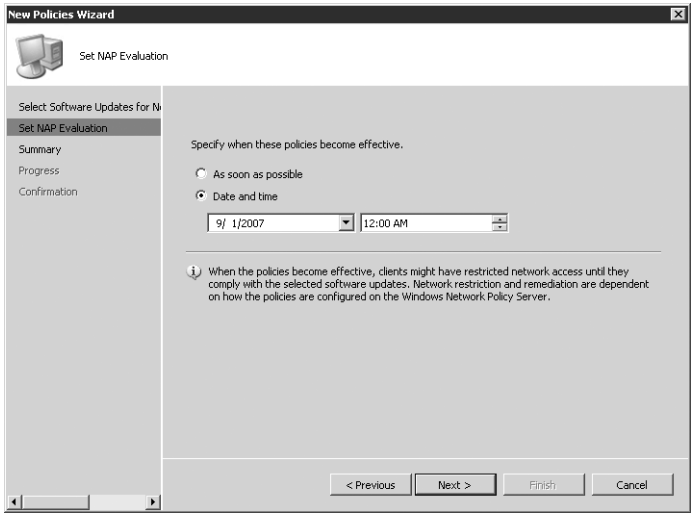


Figure 15-7 The Set NAP Evaluation page of the New Policies Wizard where you select the date to start Network Access Protection evaluation

5. Click Next, review the summary information, click Next again, and then click Close.
6. View the software updates you selected in the results pane. Each appears as a separate Network Access Protection policy with the same Effective Date, similar to Figure 15-5.

If you want to modify the Effective Date of one or more Network Access Protection policies, select them, right-click, and then select Properties. Make the modification and click OK. Figure 15-8 shows the Properties dialog box of a sample Network Access Protection policy.

To stop a software update from being included in Network Access Protection evaluation, simply select it and then press Delete. This action doesn't remove the software update from Configuration Manager or affect existing software update deployments that reference

the software update. It simply means the software update will no longer be included in Network Access Protection evaluation.

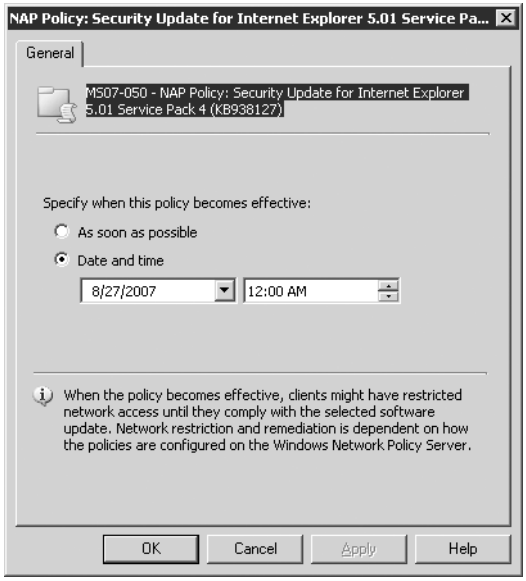


Figure 15-8 The Network Access Protection Policy Properties dialog box

The Network Access Protection policy that you see when using the Policies node is actually an attribute of the downloaded software update. This becomes more obvious if you view the properties of a software update in Update Repository under the Software Updates node. When the Network Access Protection client agent is enabled, a new tab called NAP Evaluation appears for each downloaded software update. Figure 15-9 shows an example of a software update's Properties dialog box with this NAP Evaluation tab.

As an alternative to creating Network Access Protection policies using the Policies node, you can use this tab to select the option NAP Evaluation and then configure the Effective Date. And similarly, if you created a Network Access Protection policy using the New Policies Wizard, you could delete the policy by clearing the Enable NAP Evaluation option on the software update's NAP Evaluation tab. Refreshing the Policies node will reflect your changes.

The NAP Evaluation tab also appears as a property of a software update deployment and of a software update package.

Additionally, the software updates wizards also include an NAP Evaluation page when the Network Access Protection client agent is enabled. This means that you can download

a software update with the Deploy Software Update Wizard or create a software update deployment with the Deploy Software Update Wizard, and at the same time, mark the software updates for NAP evaluation.

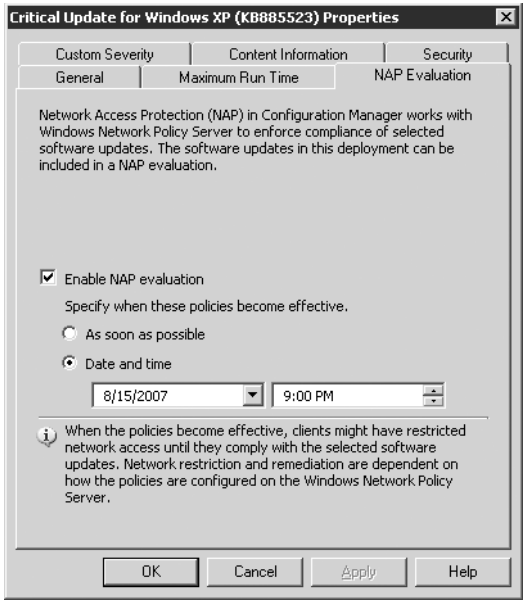


Figure 15-9 The NAP Evaluation tab of a downloaded software update

There really is no right or wrong way to mark a software update to be included in Network Access Protection evaluation. All rivers lead to the same sea. Choose the method that best suits your working practices.

Monitoring Network Access Protection

On a computer that supports Network Access Protection, the Windows client Network Access Protection notification displays when a computer has limited network access because it is noncompliant. As shown in Figure 15-10, the Network Access Protection shield displays yellow with a warning exclamation, and the network adapter icon also has a warning symbol against it to denote a network connectivity issue. In comparison, Figure 15-11 shows the Windows Network Access Protection notification a user sees when their computer is noncompliant, but does not have limited network access, and instead remediates on the full network. In this scenario, the computer has full network access for a limited time, and so the network adapter still displays the warning symbol because network connectivity is in doubt if the computer remains noncompliant after the specified time.

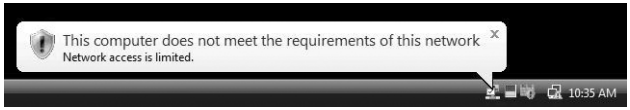


Figure 15-10 The Windows client Network Access Protection notification of a noncompliant computer with limited network access

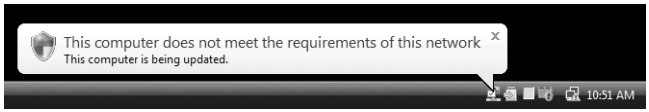


Figure 15-11 The Windows client Network Access Protection notification of a noncompliant computer with full network access for a limited time, automatically remediating

Figure 15-12 shows the Network Access Protection notification after remediation has successfully completed. The Network Access Protection shield has changed to green with a tick, and the network adapter no longer has the warning symbol.

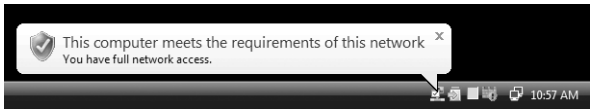


Figure 15-12 The Windows client Network Access Protection notification when a noncompliant computer has been successfully remediated

If a user clicks the Network Access Protection notification, the Windows client Network Access Protection dialog box shows the active system health agents and their current status. As with the Windows client Network Access Protection notification, this dialog box is called by Windows Network Access Protection and is not part of the Configuration Manager interface, although it displays information from the Configuration Manager System Health Agent.

The Windows Network Access Protection dialog box can be branded with your choice of title, description, and image using Group Policy. Figure 15-13 shows an example Windows Vista Network Access Protection dialog box on the client, which is not branded. The example shows the Configuration Manager System Health Agent, with the client undergoing remediation for software updates.

If remediation fails, this dialog box can provide useful troubleshooting information for the help desk, because it will show which system health agent experienced the error with related error information. Some errors result in two new buttons displayed in this dialog box: a Try Again button and a More Information button. If users click More Information, their default Web browsers connect to the troubleshooting Web site configured in the network policy. The Try Again button generates a new statement of health and is only available to users with administrator rights. This might be applicable if automatic

remediation fails and the user manually remediates on the restricted network and then needs to update the health status to move onto the unlimited network. A user without administrator rights can achieve the same result by restarting the computer after the completion of the manual remediation.

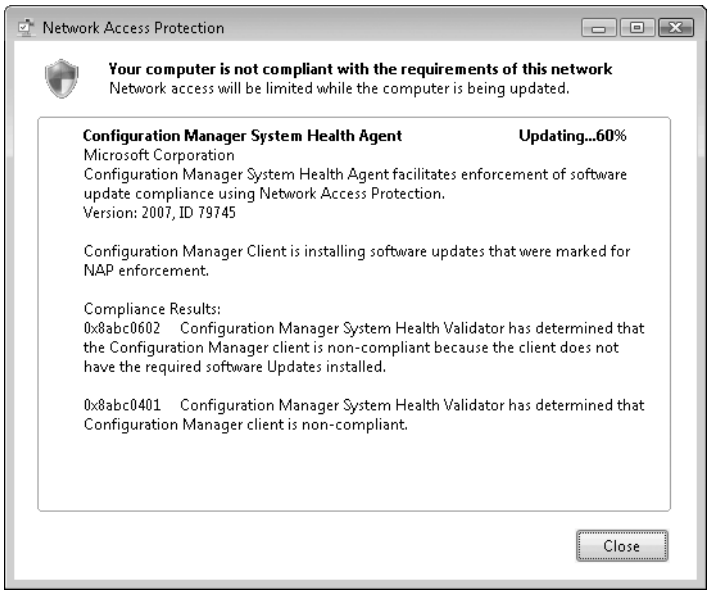


Figure 15-13 The Client Network Access Protection dialog box displaying a noncompliant computer undergoing remediation for Configuration Manager Network Access Protection

Figure 15-14 shows an example of the Network Access Protection dialog box when remediation is successful, and Figure 15-15 shows an example of unsuccessful remediation. The unsuccessful remediation in Figure 15-15 is the result of the Configuration Manager client not being installed, which was covered earlier in the section "Identify Users and Computers That Need Exemptions." When the Configuration Manager client is not installed but the NAP health policy server is expecting a statement of health from Configuration Manager, the Windows Network Access Protection dialog box is unable to map the required system health agent to a friendly name. Instead, it displays the system health agent ID that is sent from the NAP health policy server. In the case of the Configuration Manager System Health Agent, this ID is 79745.

Note The error condition shown in Figure 15-15 is one of the most commonly reported scenarios for failed Network Access Protection remediation on a network running Configuration Manager. If a user reports a "SHA Not Present" error message with ID 79745, you must either install the Configuration Manager

client on their computer, or reconfigure policies on the NAP health policy server so that their computer is exempt from Configuration Manager Network Access Protection evaluation.

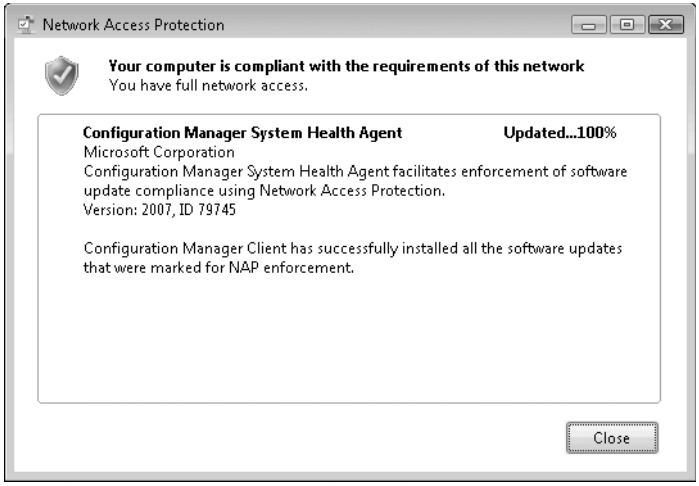


Figure 15-14 The Client Network Access Protection dialog box displaying a successfully remediated computer

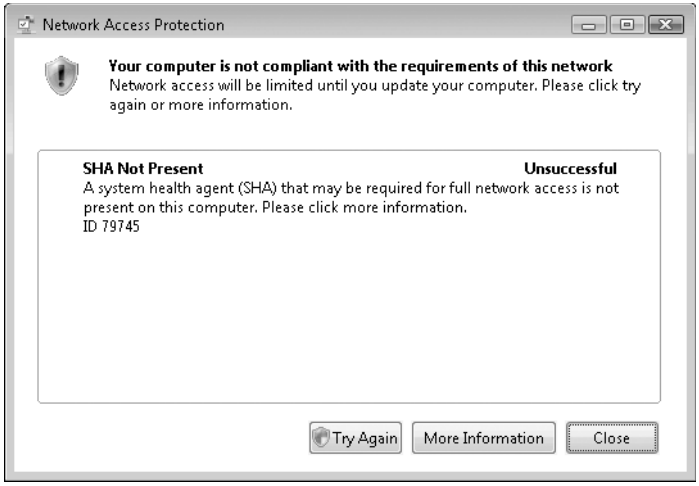


Figure 15-15 The Client Network Access Protection dialog box displaying an unsuccessfully remediated computer

More detailed client information about Network Access Protection can be obtained by running the following command from a command prompt: `NETSH NAP CLIENT SHOW STATE`.

This provides a lot of information that you might want to redirect to a file so that you can search through it more easily. The output includes the following information:

- Network Access Protection status (for example, enabled) and restriction state (for example, not restricted)
- Enforcement client states, listing each enforcement client by ID and vendor, and whether it is initialized
- System health agent states, listing the details of each including the ID (the Configuration Manager System Health Agent has ID 79745), remediation state and percentage complete (if in remediation), and compliance results

The following shows an extract of this command's output for the Configuration Manager System Health Agent section.

```
Id                      = 79745
Name                    = Configuration Manager System Health Agent
Description             = Configuration Manager System Health Agent facilitates
enforcement of software update compliance using Network Access Protection.
Version                 = 2007
Vendor name             = Microsoft Corporation
Registration date       = 8/17/2007 4:03:22 PM
Initialized             = Yes
Failure category        = None
Remediation state       = Success
Remediation percentage = 100
Fixup Message           = (90701) The Configuration Manager System Health Agent is
 compliant with the required software updates.
Compliance results      = (0x00000000) - (null)

Remediation results     = (0x00000000) - (null)
```

If you have administrator rights, you can run this command at any time on an NAP-capable client. Together with the client notification and Network Access Protection dialog box, these are useful informational and troubleshooting tools to find out how Network Access Protection is operating on individual computers. However, you need a different method to centrally monitor Network Access Protection activity for multiple Configuration Manager clients.

Using the Network Access Protection Home Page to Monitor Network Access Protection

One of the easiest ways to centrally monitor Network Access Protection activity is to use the Network Access Protection home page from the Network Access Protection node. Figure 15-16 shows an example home page with Network Access Protection activity.

One of the slightly disconcerting things about this home page is that it does not offer confirmation that Network Access Protection is working when all the clients are compliant.

It only lists "bad news" information in that it provides a count of how many computers were in remediation (on the restriction network or unlimited network), the most frequently requested software updates needed for remediation, and the most frequently occurring remediation errors.

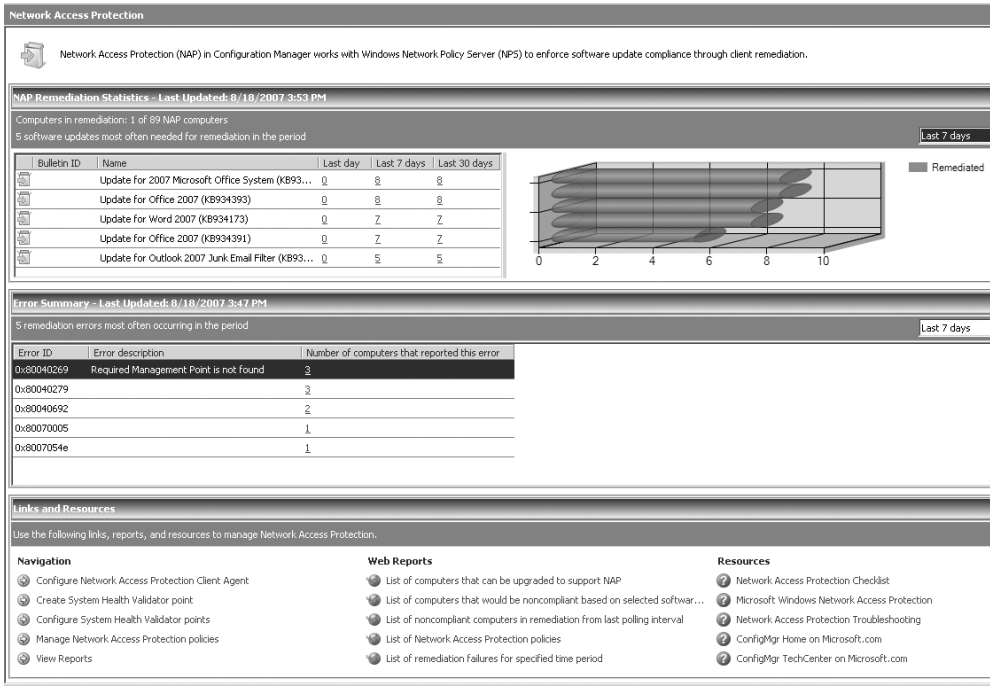


Figure 15-16 The Network Access Protection home page showing sample activity

While this snapshot information is very useful, it is important to remember that it is not real time. The information is retrieved from the database with the summarization schedule, which by default is every 30 minutes for this home page. You can change this schedule by clicking the Schedule home page summarization in the actions pane, and you can request that the data is updated ad hoc with the Run Home Page Summarization in the actions pane. However, this last request will take some time to complete, and you must refresh the screen to see the latest data. Reference the last updated value displayed to know at what time the information displayed was current. In addition, the count of Network Access Protection computers displayed in the Network Access Protection Remediation Statistics is taken from the latest hardware inventory information. This is useful in displaying how many computers assigned to the site are capable of supporting Network Access Protection without having to reference the reports.

The one unusual characteristic about this home page that is different from other home pages in Configuration Manager is that the count of computers in remediation is not

restricted to Configuration Manager remediation. If you are using other system health agents (for example, the Windows System Health Agent and System Health Validator) and Configuration Manager clients are remediated because they are noncompliant with their policies (for example, the client is not configured with an antivirus software), this will be registered in the count of computers in remediation. Do not assume that the count of computers in remediation equates to computers being remediated for Configuration Manager.

Using Reports to Monitor Network Access Protection

The following Network Access Protection reports offer more detailed information to help you to monitor Network Access Protection usage for the site:

- List of software updates installed through remediation
- Comparison of software updates installed by software update deployments and Network Access Protection remediation
- List of computers that installed a specific software update through remediation during a specified period
- List of noncompliant computers in remediation from last polling interval
- List of noncompliant computers in remediation within a specified period
- Summary of noncompliant computers in remediation from last polling interval
- Summary of noncompliant computers in remediation within a specified period
- Frequency a computer has been in remediation within a specified period

Additionally, use the following report to help you identify any failures that occur during remediation:

- List of remediation failures for specified time period

You can also use the following reports for planning, to help you identify which clients in the site can support Network Access Protection and which could be upgraded with the Network Access Protection client for Windows XP:

- List of computers that can be upgraded to support Network Access Protection
- List of NAP-capable and NAP-upgradable computers

You can use the following report as a "what if" mechanism to find out how many computers would be liable to remediation based on selected software updates:

- List of computers that would be noncompliant based on selected software updates

And to help you record and identify which software updates are selected for Network Access Protection (particularly if you are creating Network Access Protection policies using the software update wizards), use the following report:

- List of Network Access Protection policies

Using Performance Counters and Event Logs to Monitor Network Access Protection

Installing the System Health Validator point automatically installs some Windows performance counters for the object Configuration Manager System Health Validator. Use this for each System Health Validator point to monitor validation activity. For example, by monitoring the counter SoH Requests Total, you can confirm that the Configuration Manager Network Access Protection infrastructure is working. Configuration Manager clients that are capable of supporting Network Access Protection will send a statement of health (SoH) even if the Configuration Manager Network Access Protection client agent is disabled, and even if no software updates are marked for Network Access Protection. So this counter provides a useful confirmation that the System Health Validator point is working.

Other useful counters include SoH Response: Compliant and SoH Response: Noncompliant to monitor the number of compliant and noncompliant clients. Also, remembering that noncompliant doesn't necessarily mean that software updates were missing, reference the counter Software Updates Not Installed to determine how often clients were remediated with software updates. You can reference the full list of performance counters and a description of each in the topic "How to Monitor the System Health Validator Point with Performance Counters for Network Access Protection" from the Configuration Manager documentation library.

Additionally, entries for the SMS_SYSTEM_HEALTH_VALIDATOR appear in the Windows Application log on the NAP health policy server.

Using Log Files to Monitor Network Access Protection

If you need more nitty-gritty details (for example, to confirm each component is working or to troubleshoot a problem), log files on clients and the Network Access Protection policy server provide this level of detail. For a list of log files related to Network Access Protection, see the topic "Log Files for Network Access Protection" in the Configuration Manager 2007 documentation library. Additionally, to find which log file and the entries to search for to verify Network Access Protection components, see "How to Verify Network Access Protection Components."

Checkpoints for Phasing in Network Access Protection

In addition to testing in a lab environment, it pays to be cautious when implementing Network Access Protection on a production network. Consider baby steps before

jumping in and enabling Network Access Protection on all sites with limited access for noncompliant computers.

You should always implement Network Access Protection in Configuration Manager in a top-down approach, enabling it first on your central site or wherever you synchronize your software update point with the Microsoft Windows Update site. However, enable it carefully one site at a time, noting the number of NAP-capable clients in each as a measure of its potential reach.

Second, although Network Access Protection in Configuration Manager cannot remediate in reporting mode, consider this configuration as a pilot and confirm that the Network Access Protection components are working as expected. Then enable the option for full network access for a limited time, specifying a date and time comfortably in the future so that there is no chance of noncompliant computers having restricted network access. This tests remediation on the full network, and although users will not see the Network Access Protection notification, you can use the Configuration Manager reports and Network Access Protection home page to monitor remediation activity.

Because remediating on the full network for a limited time brings about compliance without loss of network connectivity, some customers might find this mode of Network Access Protection operation more productive and less risky than enforcing compliance with limited network access. However, it does not help to prevent noncompliant computers from accessing network resources, so you need to balance this risk with the risk of loss of business continuity from anything from a few minutes to indefinitely (for example, the client's management point is not operational, or there is a network failure between the client and distribution points needed for remediation).

Finally, when you have proved that noncompliant computers are successfully remediated within an acceptable time frame, and all the help desk processes are in place to deal with calls from users who do not have network access, enable restriction of noncompliant computers with the option of limited network access.

Note If you ever need an emergency Off button for Configuration Manager Network Access Protection because computers indefinitely fail to gain full network access (for example, all computers experience an unrecoverable Network Access Protection failure), the most expedient method is not to disable Network Access Protection in Configuration Manager, but to change the network policies on the NAP health policy server such that they no longer include health policies for the Configuration Manager System Health Validator. Then restart the computers that cannot get full network access.

Summary

This chapter introduced you to the underlying architecture that Network Access Protection in Configuration Manager depends upon to enforce compliance of software updates for clients that can support Network Access Protection. It took you through the careful planning that must go into a deployment of Network Access Protection, how to install and configure the System Health Validator point on the NAP health policy server, and how to configure the Network Access Protection client agent for NAP-enabled sites. You looked at the different ways in which you can create Network Access Protection policies in Configuration Manager and how to monitor them and Network Access Protection activity for the site.

For detailed information about how to implement Network Access Protection on Windows Server 2008, see the Windows Network Access Protection Web site for current documentation and information, as well as the book titled *Windows Server 2008 Networking and Network Access Protection (Network Access Protection)* (Microsoft Press, 2008).