



Windows Server[™] 2008



Network Access Protection Policies in Windows Server 2008

Microsoft Corporation

Published: February 2006

Updated: February 2008

Abstract

A network administrator configures Network Access Protection (NAP) health policies and enforcement behavior on a computer running Microsoft[®] Windows Server[®] 2008 and the Network Policy Server (NPS) service. NAP health policies and enforcement behavior settings consist of connection request policies, network policies, health policies, and Network Access Protection settings, each of which play a role in determining the health state of a computer and limiting the access of noncompliant computers. This paper describes the different settings of NPS for NAP in Windows Server 2008 and how the different settings are related to create a customized health determination and enforcement solution.

Microsoft[™]

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2008 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

Introduction	1
RADIUS Clients.....	2
NAP Settings for Health Determination and Enforcement.....	2
NAP Settings for Health Determination and Enforcement in NPS	4
Connection Request Policies	4
Health Policies	5
Network Access Protection Settings	6
System Health Validators	6
Remediation Server Groups.....	8
Network Policies	8
Access Permission Setting for NAP	8
Network Policy Conditions for NAP	9
Network Policy Settings for NAP	9
How NAP Health Evaluation Works	12
Examples of Health Evaluation Processing for NAP	13
NPS Processing for a Compliant NAP Client.....	14
NPS Processing for a Noncompliant NAP Client	14
NPS Processing for a NAP Ineligible Client	15
Summary	16
Related Links	17

Introduction

Network Access Protection (NAP) is a system health policy enforcement platform built into Windows Server 2008, Windows Vista™, and Windows® XP [Service Pack 3](#), that allows you to control access to network resources based on a client computer's identity and compliance with corporate governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

For an overview of NAP, see the [Introduction to Network Access Protection](#) white paper at <http://go.microsoft.com/fwlink/?LinkId=49884>. For additional resources, see the [Network Access Protection Web site](#) at <http://www.microsoft.com/nap>.

The central server that performs the health evaluation is a NAP health policy server, a computer running Windows Server 2008 and Network Policy Server (NPS). NPS is the Windows implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy. NPS is the replacement for the Internet Authentication Service (IAS) in Windows Server 2003. RADIUS is an Internet Engineering Task Force (IETF) standard specified in Requests for Comments (RFCs) 2865 and 2866. Network access devices and NAP enforcement points act as RADIUS clients to an NPS-based RADIUS server. NPS performs authentication and authorization of a network connection attempt and, based on configured system health policies, evaluates computer health compliance and determines how to limit a noncompliant computer's network access or communication.

To configure a NAP health policy server for health determination and enforcement behaviors for NAP enforcement points, you must configure RADIUS clients and NAP settings for health determination and enforcement.

This paper does not describe the steps for configuring health requirement policies for each of the NAP enforcement methods. For examples, see the following:

- [Step-by-Step Guide: Demonstrate IPsec NAP Enforcement in a Test Lab](#) at <http://www.microsoft.com/downloads/details.aspx?FamilyID=298ff956-1e6c-4d97-a3ed-7e7ffc4bed32&displaylang=en>
- [Step By Step Guide: Demonstrate 802.1X NAP Enforcement in a Test Lab](#) at <http://www.microsoft.com/downloads/details.aspx?FamilyID=8a0925ee-ee06-4dfb-bba2-07605eff0608&displaylang=en>
- [Step-by-Step Guide: Demonstrate VPN NAP Enforcement in a Test Lab](#) at <http://www.microsoft.com/downloads/details.aspx?FamilyID=729bba00-55ad-4199-b441-378cc3d900a7&displaylang=en>
- [Step-by-Step Guide: Demonstrate DHCP NAP Enforcement in a Test Lab](#) at <http://www.microsoft.com/downloads/details.aspx?FamilyID=ac38e5bb-18ce-40cb-8e59-188f7a198897&displaylang=en>

RADIUS Clients

You must add a RADIUS client for each NAP enforcement point that is separate from the NAP health policy server. Examples of NAP enforcement points include IEEE 802.1X-based wireless access points and authenticating switches, virtual private network (VPN) servers running Windows Server 2008, Dynamic Host Configuration Protocol (DHCP) servers running Windows Server 2008, and Health Registration Authorities (HRAs) running Windows Server 2008.

To add a NAP enforcement point as a RADIUS client to an NPS server, open **RADIUS Clients and Servers** in the console tree of the Network Policy Server snap-in, right-click **RADIUS Clients**, and then click **New RADIUS Client**. The **New RADIUS Client** dialog box allows you to configure the settings for the RADIUS client. In the **New RADIUS Client** dialog box, select the **Client is NAP-capable** check box for NAP enforcement points except for IEEE 802.1X-based wireless access points and authenticating switches. Figure 1 shows an example.

Figure 1: The New RADIUS Client dialog box

NAP Settings for Health Determination and Enforcement

NAP settings for health determination and enforcement consist of the following sets of settings:

- Connection request policies
- Network policies
- Health policies
- Network Access Protection settings

Health requirement policies on the NAP health policy server determine whether a NAP-capable client is compliant or noncompliant, how to treat noncompliant NAP clients and whether they should automatically remediate their health state, and how to treat non-NAP-capable clients for different NAP enforcement methods. A health requirement policy is a combination of a connection request policy, a health policy, Network Access Protection settings, and a network policy. Although discussed separately in this white paper, you should configure the initial set of health requirement policies with the Configure NAP Wizard, available from the NPS node in the Network Policy Server snap-in.

The remainder of this white paper describes the details of health requirement policies and NAP settings for health determination and enforcement in NPS.

Note Network policies in NPS are equivalent to remote access policies in IAS.

NAP Settings for Health Determination and Enforcement in NPS

Connection request policies, network policies, health policies, and Network Access Protection settings correspond to different nodes in the console tree of the Network Policy Server snap-in, as Figure 2 shows.

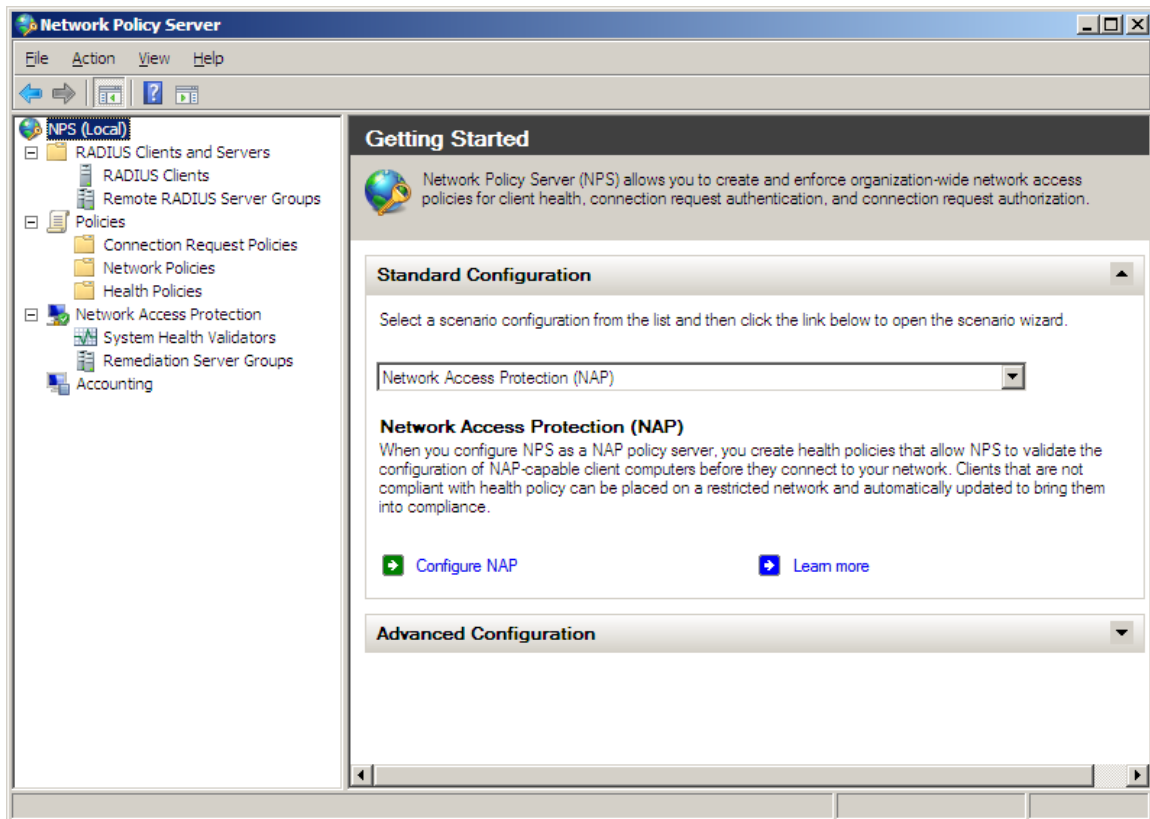


Figure 2: The Network Policy Server snap-in

Connection Request Policies

NPS in Windows Server 2008 can be used as either a RADIUS server or a RADIUS proxy. When the NPS service is used as a RADIUS server:

- RADIUS Access-Request messages are authenticated through the Active Directory® domain service, a Windows NT Server 4.0 domain, or through the local Security Accounts Manager (SAM). They are authorized with the user or computer account properties and a network policy.
- RADIUS Accounting-Request messages are logged in a local log file or a Microsoft SQL Server database, based on NPS accounting settings.

When the NPS service is used as a RADIUS proxy:

- Access-Request messages are forwarded to another RADIUS server for authentication and authorization.
- Accounting-Request messages are logged in a local log file or a Microsoft SQL Server database (based on accounting settings) and forwarded to another RADIUS server for accounting.

Connection request policies are an ordered set of rules that allow the NPS service to determine whether a specific connection attempt request or an accounting message received from a RADIUS client should be processed locally or forwarded to another RADIUS server. You can configure connection request policies from the Policies node of the Network Policy Server snap-in. When forwarding messages, you must specify a remote RADIUS server group in the connection request policy, which you can configure from the RADIUS Clients and Servers node of the Network Policy Server snap-in.

When you are configuring the NPS server to perform NAP health determination and enforcement, NPS is acting as a RADIUS server. Therefore, remote RADIUS server groups are not needed and this white paper does not describe their configuration. However, connection request policies for local processing of RADIUS request messages might need to be configured or customized for NAP health evaluation.

Health Policies

Health policies allow you to specify health requirements in terms of installed system health validators (SHVs) and whether NAP clients must pass or fail any or all of the selected SHVs. Figure 3 shows an example health policy.

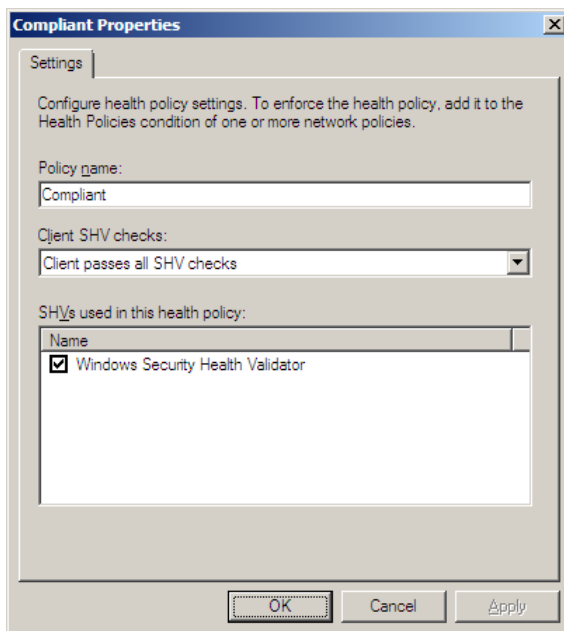


Figure 3: An example health policy

In **Policy name**, type the unique name of the policy. In **Client SHV checks**, specify one of the following:

- Client passes all SHV checks

The client's health status in the connection request must pass the health requirements for all of the SHVs selected in the **SHVs used in this health policy** list. Select this option to define a compliant computer as a NAP client that must pass the health requirements for all of the selected SHVs.

- Client fails all SHV checks

The client's health status in the connection request must fail all of the health requirements for all of the SHVs selected in the **SHVs used in this health policy** list. Select this option to define a compliant computer as a NAP client that fails the health requirements for all of the selected SHVs.

- Client passes one or more SHV checks

The client's health status in the connection request must pass the health requirements of at least one of the SHVs selected in the **SHVs used in this health policy** list. Select this option to define a compliant computer as a NAP client that must pass the health requirements of at least one SHV.

- Client fails one or more SHV checks

The client's health status in the connection request must fail the health requirements of at least one of the SHVs selected in the **SHVs used in this health policy** list. Select this option to define a compliant computer as a NAP client that fails any of the SHVs.

In the **SHVs used in this health policy** list, select the installed SHVs that apply to the policy. By default, the Windows Security Health Validator SHV is listed.

To create a new health policy, right-click **Health Policies** in the Network Policy Server console tree, and then click **New**.

Network Access Protection Settings

Network Access Protection settings consist of the following:

- **System Health Validators** Specifies the configuration of installed SHVs for health requirements and error conditions.
- **Remediation Server Groups** Specifies the set of servers that are accessible to noncompliant clients with limited network access.

Figure 2 shows the location of the Network Access Protection settings in the Network Policy Server console tree.

System Health Validators

The System Health Validators node displays the set of SHVs that are installed on the NPS server and allows you to configure their settings for health requirements and error conditions. By default, the Windows Security Health Validator is installed. Figure 4 shows the properties of the Windows Security Health Validator.

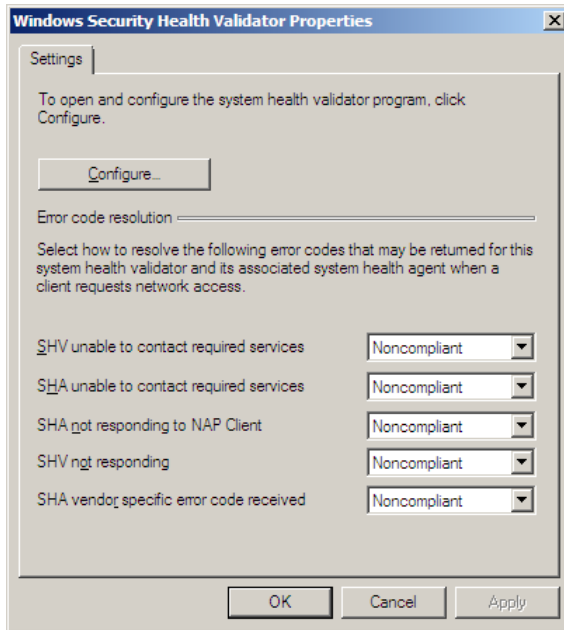


Figure 4: The Windows Security Health Validator Properties dialog box

From this dialog box, you can configure how the NPS service interprets various error conditions. To configure the health requirements for the Windows Security Health Validator SHV, click **Configure**. Figure 5 shows the default **Windows Security Health Validator** dialog box.

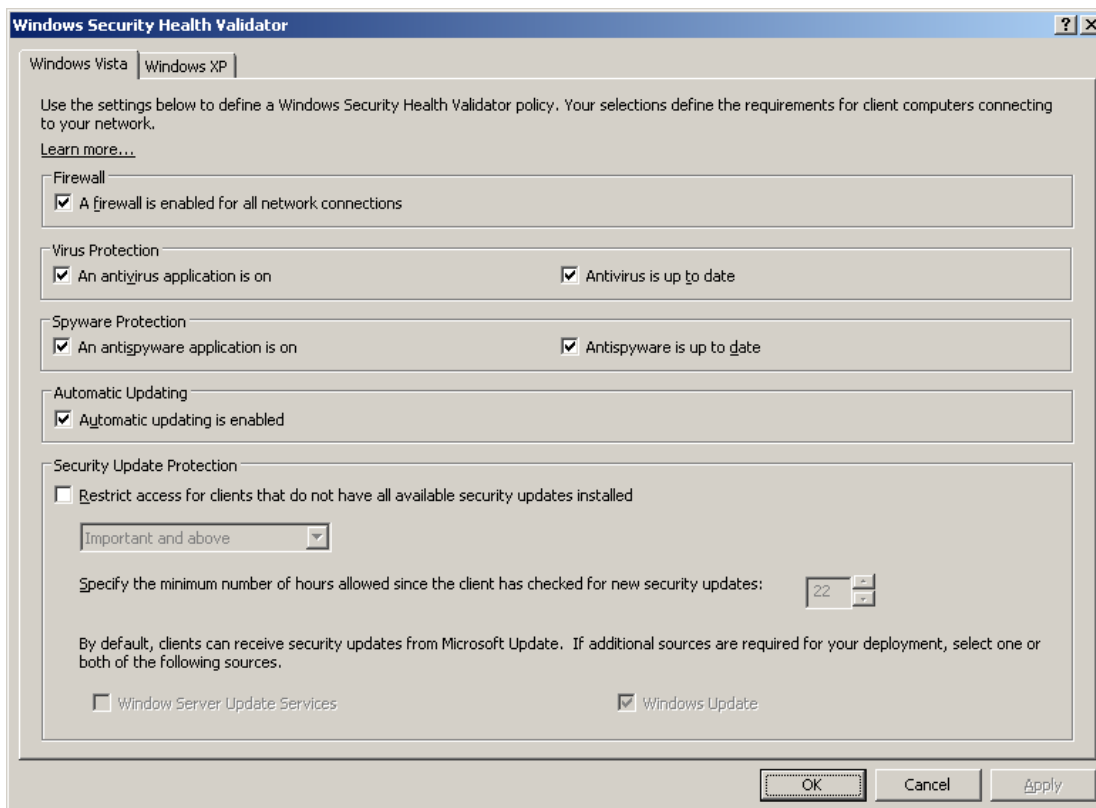


Figure 5: The Windows Security Health Validator dialog box

From this dialog box, you can select the health requirements for NAP clients for built-in Windows services that are monitored by the Windows Security Center in Windows Vista (from the **Windows Vista** tab) and Windows XP with Service Pack 3 (from the **Windows XP** tab).

Remediation Server Groups

A remediation server group is a list of servers that noncompliant NAP clients or non-NAP-capable clients can access. You might have separate groups for noncompliant NAP clients or non-NAP-capable clients or separate groups for different NAP enforcement methods.

To create a new remediation server group, right-click **Remediation Server Groups** in the Network Policy Server console tree, and then click **New**. From the **New Remediation Server Group** dialog box, you can specify remediation servers by Domain Name System (DNS) name, IPv4 address, or IPv6 address. Figure 6 shows an example.

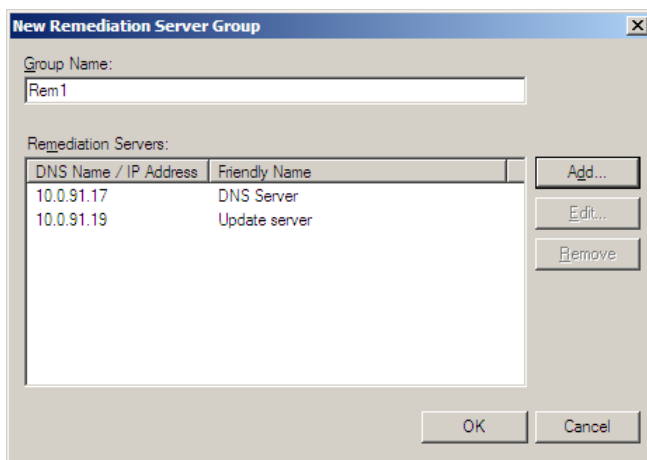


Figure 6: The New Remediation Server Group dialog box

Network Policies

Network policies are an ordered set of rules that define how connection attempts are either authorized or rejected. For each rule, there is an access permission that either grants or denies access, a set of conditions, a set of constraints, and network policy settings. If a connection is authorized, the network policy constraints and settings can specify a set of connection restrictions. For NAP, network policies specify the conditions to check for health requirements and, for noncompliant NAP clients or non-NAP-capable clients, the enforcement behavior.

Access Permission Setting for NAP

Whether or not NAP health validation is being done for connection attempts that are also authenticated and authorized, you select **Grant access** for the access permission. The connection attempt is authorized, but the network access of noncompliant NAP clients or non-NAP-capable clients can be limited to the remediation servers. You can create network policies to explicitly deny access; however, these network policies do not need NAP settings as it is not necessary to validate the system health of a computer that is not allowed access.

Network Policy Conditions for NAP

For NAP support, the following conditions have been added to NPS network policies:

- Health Policy
Specifies a previously configured health policy. If the health settings of a connection attempt match the health policy, the connection attempt matches this condition of the network policy.
- NAP-Capable
Specifies whether the client is NAP capable or not.
- Policy Expiration
Specifies when the network policy expires and is no longer evaluated. You can use this to transition from a reporting mode to an enforcement mode of NAP operation.

The following are examples of using the Health Policy and NAP-Capable conditions for NAP-based network policies:

- For a network policy that applies only to compliant NAP capable clients that pass all of the health requirements of the installed SHVs, specify the following condition:
 - Set the Health Policy condition to the "Compliant" (example name) health policy, which specifies the **Client passes all SHV checks** option.
- For a network policy that applies only to noncompliant NAP capable clients that fail any of the health requirements of the installed SHVs, specify the following condition:
 - Set the Health Policy condition to the "Noncompliant" (example name) health policy, which specifies the **Client fails one or more SHV checks** option.
- For a network policy that applies only to non-NAP-capable clients, specify the following condition:
 - Set the NAP-Capable condition to **Only computers that are not NAP-capable**.

Network Policy Settings for NAP

Network policies in Windows Server 2008 have a set of network policy settings for NAP Enforcement. Figure 7 shows an example.

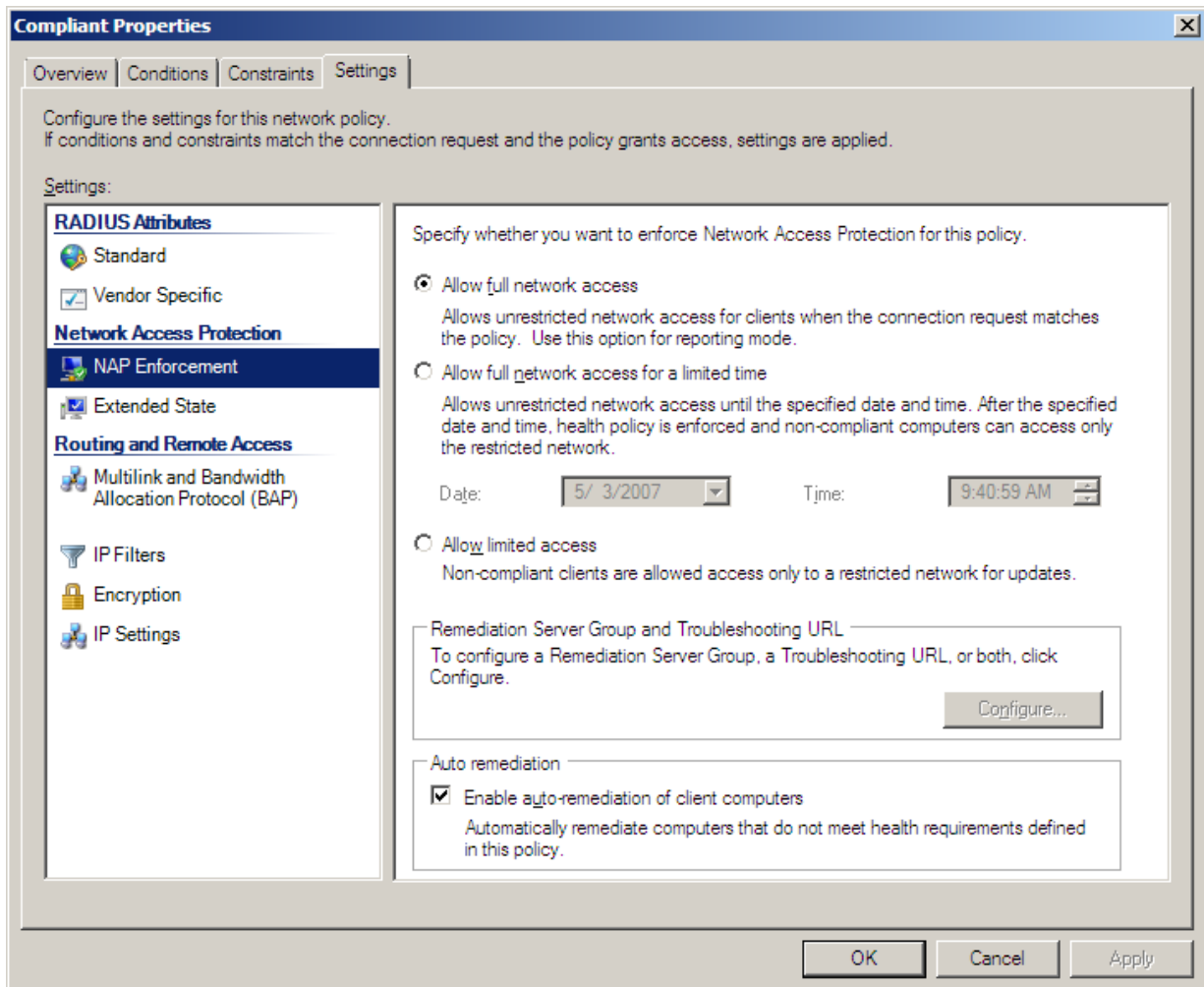


Figure 7: NAP Enforcement settings

For NAP Enforcement settings, you can specify the following:

- **Allow full network access** Specifies that the connection attempt has unlimited network access. Select this option for network policies defined for compliant NAP clients.
- **Allow full network access for a limited time** Specifies that the connection attempt has unlimited network access, but users on noncompliant NAP client computers receive a notification message that they must become compliant by the configured date and time. This is also known as *deferred enforcement mode*.
- **Allow limited access** Specifies that the connection attempt has limited network access. Select this option for network policies defined for noncompliant NAP clients or for non-NAP-capable clients.
- **Enable auto-remediation of client computers** Specifies that the connection attempt has limited network access. Users on noncompliant NAP client computers receive a “This computer is not compliant with the requirements of this network” notification message. This is also known as *enforcement mode*.

For limited access, click **Configure** to specify the remediation server group and troubleshooting URL. Figure 8 shows the **Remediation Servers and Troubleshooting URL** dialog box.

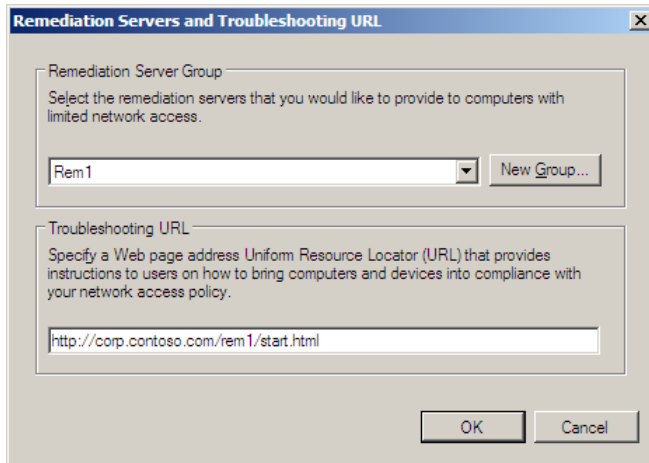


Figure 8: Remediation Servers and Troubleshooting URL dialog box

In **Remediation Server Group**, select a previously configured remediation server in the list or click **New Group** to create a new remediation server group.

In **Troubleshooting URL**, type the URL to a Web page of a remediation server for noncompliant NAP clients. This URL is activated when a user clicks **Troubleshoot** on the **Network Access Protection** dialog box that is displayed on noncompliant NAP clients. From the Web page, the user can determine how to update the computer so that it is compliant or perform troubleshooting of network access. This URL is also visible in the display of the **netsh nap client show state** command on the noncompliant NAP client.

How NAP Health Evaluation Works

The process that the NPS service on the NAP health policy server uses to perform health evaluation is the following:

1. When the NPS service on the NAP health policy server receives the RADIUS Access-Request message from a NAP enforcement point, it first determines whether the message originated from an address that corresponds to a configured RADIUS client. If not, the NPS service discards the message. This behavior prevents the NAP health policy server from processing RADIUS messages from RADIUS clients (such as access devices and NAP enforcement points) for which the NPS service has not been configured.
2. The NPS service then compares the Access-Request message to its configured set of connection request policies. For NAP, the Access-Request message should match a connection request policy that specifies that the NPS service perform the authentication and authorization locally.
3. The NPS service evaluates the health information in the Access-Request message, which consists of a system statement of health (SSoH) containing one or more statements of health (SoHs). The NAP Administration Server component on the NAP health policy server passes each SoH to the appropriate SHV for evaluation. The result of the evaluation is a set of statement of health responses (SoHRs) from the SHVs.
4. The NPS service evaluates the Access-Request message and the SoHRs against the network policies. The SoHRs are compared to the Health Policy condition of NAP-based network policies. Recall that the Health Policy condition specifies whether the SHVs must either pass or fail. The NPS service applies the best matching network policy to the Access-Request message. The best matching network policy is either the first matching network policy with a specific source (for Access-Request messages that specify a source tag indicating the type of RADIUS client) or the first matching network policy with an unspecified source (for Access-Request messages that do not specify a source tag).
5. Based on the best matching network policy and the Network Access Protection settings of that policy, the NPS service creates a system statement of health response (SSoHR), which includes the SoHRs from the SHVs and indicates one of the following:
 - The client has unlimited access.
 - The client has limited access. In this case, the SSoHR also includes whether the client should automatically attempt to remediate its noncompliant health state.
6. The NPS service sends a RADIUS Access-Accept message with the SSoHR to the NAP enforcement point that sent the Access-Request message. If the client has limited access, the Access-Accept message can also contain the list of addresses for the remediation servers corresponding to the configured remediation server group.
7. The NAP enforcement point sends the SSoHR to the NAP client.

Note The details of steps 6 and 7 depend on the enforcement method and the NAP enforcement point. In some cases, the NPS service sends both the SSoHR and the limited access instructions to the NAP enforcement point, as is described in steps 6 and 7. In some cases, the NPS service sends the SSoHR to the NAP client and the limited access instructions to the NAP enforcement point.

Examples of Health Evaluation Processing for NAP

The following sections describe how the NPS service processes incoming Access-Request messages for access attempts from three different types of clients (a compliant NAP client, a noncompliant NAP client, and a non-NAP-capable client) based on the following configuration:

- Connection request policies

NPS uses the default connection request policy **Use Windows authentication for all users**, which causes the NPS service to process all RADIUS messages locally, rather than forwarding them to another RADIUS server.

- Network Access Protection settings

The Windows Security Health Validator is configured to only require that automatic updating be enabled on NAP clients.

A health policy named MSSHV_Compliant specifies the use of the Windows Security Health Validator SHV and the **Client passes all SHV checks** option.

A health policy named MSSHV_Noncompliant specifies the use of the Windows Security Health Validator SHV and the **Client fails all SHV checks** option.

A remediation server group named REM1 contains a list of the IPv4 addresses for the remediation servers.

- Network policies

A network policy named Compliant_NAP_clients is configured for the following:

- Conditions: Health Policy is set to the MSSHV_Compliant policy
- Settings: For NAP Enforcement, the **Allow full network access** option is selected

A network policy named Noncompliant_NAP_clients is configured for the following:

- Conditions: Health Policy is set to the MSSHV_Noncompliant policy
- Settings: For NAP Enforcement, the **Allow limited access** option is selected, the REM1 remediation server group is selected for the remediation server group, and auto-remediation of client computers is enabled

A network policy named Downlevel_clients is configured for the following:

- Conditions: NAP-Capable is set to **Only computers that are not NAP-capable**
- Settings: For NAP Enforcement, the **Allow limited access** option is selected, and for the remediation server group, the REM1 remediation server group is selected

NPS Processing for a Compliant NAP Client

When a compliant NAP client (for our example, a client that has automatic updating enabled) attempts to obtain an IP address configuration from a NAP-capable DHCP server, the following process occurs:

1. The NAP client sends the DHCP server its SSoH containing the SoH from the Windows Security Health Agent SHA that indicates that automatic updating is enabled.
2. The DHCP server sends the NAP health policy server an Access-Request message containing the SSoH.
3. The NPS service on the NAP health policy server evaluates the Access-Request message against the connection request policies and matches the **Use Windows authentication for all users** connection request policy.
4. The NPS service evaluates system health by passing the SoH to the Windows Security Health Validator SHV, which returns an SoHR that indicates that the SoH meets system health requirements.
5. The NPS service evaluates the Access-Request message and the SoHR against the network policies.
6. The Access-Request message and the SoHR match the Compliant_NAP_clients network policy because the Health Policy condition, set to the MSSHV_Compliant policy, requires that the request pass all the selected SHVs (the Windows Security Health Validator SHV).
7. Based on the Network Access Protection settings of the Compliant_NAP_clients network policy (set to **Allow full network access**), the NPS service creates an SSoHR indicating unlimited access and containing the SoHR from the Windows Security Health Validator SHV.
8. The NAP health policy server sends an Access-Accept message to the DHCP server containing the SSoHR.
9. The DHCP server assigns an unlimited access IP address configuration to the NAP client. During the DHCP message exchange, the DHCP server also passes the SSoHR to the NAP client.

NPS Processing for a Noncompliant NAP Client

When a noncompliant NAP client (for our example, one that has automatic updating disabled) attempts to obtain an IP address configuration from a NAP-enabled DHCP server, the following process occurs:

1. The NAP client sends the DHCP server its SSoH, which contains the SoH from the default Windows Security Health Agent SHA that indicates that automatic updating is disabled.
2. The DHCP server sends the NAP health policy server an Access-Request message containing the SSoH.
3. The NPS service on the NAP health policy server evaluates the Access-Request message against the connection request policies and matches the **Use Windows authentication for all users** connection request policy.
4. The NPS service evaluates system health by passing the SoH to the Windows Security Health Validator SHV, which returns an SoHR indicating that the system health requirements failed.
5. The NPS server evaluates the Access-Request message and the SoHR against the network policies.

6. The Access-Request message and the SoHR match the Noncompliant_NAP_clients network policy because the Health Policy condition, set to the MSSHV_Noncompliant policy, requires that the request fail all the selected SHVs (the Windows Security Health Validator SHV).
7. Based on the Network Access Protection settings of the Noncompliant_NAP_clients network policy (set to **Allow limited access** with the REM1 remediation servers group), the NPS service creates an SSoHR indicating limited access and containing the SoHR from the Windows Security Health Validator SHV.
8. The NAP health policy server sends an Access-Accept message to the DHCP server containing the SSoHR and the list of addresses in the REM1 remediation server group.
9. Because the SSoHR indicates limited access, the DHCP server assigns a limited IP address configuration to the NAP client. During the DHCP message exchange, the DHCP server also passes the SSoHR to the NAP client.

NPS Processing for a NAP Ineligible Client

When a non-NAP-capable client attempts to obtain an IP address configuration from a NAP-enabled DHCP server, the following process occurs:

1. The DHCP server sends the NAP health policy server an Access-Request message.
2. The NPS service on the NAP health policy server evaluates the Access-Request message against the connection request policies and matches the **Use Windows authentication for all users** connection request policy.
3. The NPS service evaluates the Access-Request message against the network policies.
4. The Access-Request message matches the Downlevel_clients network policy because the Access-Request message is for a non-NAP-capable client.
5. Based on the Network Access Protection settings of the Downlevel_clients network policy (set to **Allow limited access** with the REM1 remediation servers group), the NPS service creates an SSoHR indicating limited access.
6. The NAP health policy server sends an Access-Accept message to the DHCP server containing the SSoHR and the list of IP addresses in the REM1 remediation server group.
7. Because the SSoHR indicates limited access, the DHCP server assigns a limited IP address configuration to the non-NAP-capable client.

Summary

Configuring the NPS service in Windows Server 2008 as a NAP health policy server consists of creating RADIUS clients and configuring connection request policies, health policies, Network Access Protection settings, and network policies. When processing a RADIUS Access-Request message for a connection attempt, the NPS service first uses connection request policies to determine whether to process the connection attempt locally or forward it to another RADIUS server. The NPS service then attempts to match the connection attempt with a network policy. For health validation on connection attempts, network policy conditions allow you to specify system health requirements and compliance (by referencing a health policy) and the type of client (NAP capable or non-NAP-capable). Network Access Protection settings in network policies allow you to specify enforcement behavior for noncompliant NAP clients and non-NAP-capable clients.

Related Links

See the following resources for further information:

- [Microsoft Network Access Protection Web page](http://www.microsoft.com/nap) at <http://www.microsoft.com/nap>
- [Introduction to Network Access Protection](http://go.microsoft.com/fwlink/?LinkId=49884) at <http://go.microsoft.com/fwlink/?LinkId=49884>
- [Network Access Protection Platform Architecture](http://go.microsoft.com/fwlink/?LinkId=49885) at <http://go.microsoft.com/fwlink/?LinkId=49885>
- [Network Access Protection Frequently Asked Questions](http://go.microsoft.com/fwlink/?LinkId=49886) at <http://go.microsoft.com/fwlink/?LinkId=49886>

For examples of configuring health requirement policies for each of the NAP enforcement methods, see the following:

- [Step-by-Step Guide: Demonstrate IPsec NAP Enforcement in a Test Lab](http://www.microsoft.com/downloads/details.aspx?FamilyID=298ff956-1e6c-4d97-a3ed-7e7ffc4bed32&displaylang=en) at <http://www.microsoft.com/downloads/details.aspx?FamilyID=298ff956-1e6c-4d97-a3ed-7e7ffc4bed32&displaylang=en>
- [Step By Step Guide: Demonstrate 802.1X NAP Enforcement in a Test Lab](http://www.microsoft.com/downloads/details.aspx?FamilyID=8a0925ee-ee06-4dfb-bba2-07605eff0608&displaylang=en) at <http://www.microsoft.com/downloads/details.aspx?FamilyID=8a0925ee-ee06-4dfb-bba2-07605eff0608&displaylang=en>
- [Step-by-Step Guide: Demonstrate VPN NAP Enforcement in a Test Lab](http://www.microsoft.com/downloads/details.aspx?FamilyID=729bba00-55ad-4199-b441-378cc3d900a7&displaylang=en) at <http://www.microsoft.com/downloads/details.aspx?FamilyID=729bba00-55ad-4199-b441-378cc3d900a7&displaylang=en>
- [Step-by-Step Guide: Demonstrate DHCP NAP Enforcement in a Test Lab](http://www.microsoft.com/downloads/details.aspx?FamilyID=ac38e5bb-18ce-40cb-8e59-188f7a198897&displaylang=en) at <http://www.microsoft.com/downloads/details.aspx?FamilyID=ac38e5bb-18ce-40cb-8e59-188f7a198897&displaylang=en>