

[2eddb616-63a6-4682-b578-31f1bee106f2](#)

[89af7ff1-3899-4d7d-8f3d-77c33c4531b1](#)

# Step By Step Guide: Demonstrate DHCP NAP Enforcement in a Test Lab

---

Microsoft Corporation

Published: February 2008

## Abstract

Network Access Protection (NAP) is a new policy enforcement technology in the Windows Vista® and Windows Server® 2008 and Windows XP with Service Pack 3 operating systems. NAP provides components and an application programming interface (API) set that help administrators enforce compliance with health requirements for network access and communication. This paper contains an introduction to NAP and instructions for setting up a test lab to deploy NAP with the DHCP enforcement method.

[f378c4f7-3ad7-4f6a-a215-b7fc87d1afe5](#)

# Copyright Information

---

This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. 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, MS-DOS, Windows, Windows NT, and Windows Server 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

---

|  |    |
|--|----|
| Step-by-Step Guide: Demonstrate DHCP NAP Enforcement in a Test Lab ..... | 5  |
| In this guide .....  | 5  |
| Scenario overview .....  | 6  |
| NAP enforcement processes .....  | 6  |
| Policy validation.....   | 6  |
| NAP enforcement and network restriction.....                             | 7  |
| Remediation .....  | 7  |
| Ongoing monitoring to ensure compliance.....                             | 7  |
| DHCP NAP enforcement overview .....                                      | 8  |
| Hardware and software requirements .....                                 | 8  |
| Steps for configuring the test lab.....                                  | 8  |
| Configure DC1.....   | 9  |
| Install the operating system on DC1 .....                                | 9  |
| Configure TCP/IP on DC1 .....  | 10 |
| Configure DC1 as a domain controller and DNS server.....                 | 10 |
| Create a user account in Active Directory .....                          | 11 |
| Add user1 to the Domain Admins group.....                                | 11 |
| Create a security group for NAP client computers .....                   | 12 |
| Configure NPS1 .....   | 12 |
| Install Windows Server 2008 or Windows Server 2008 R2.....               | 12 |
| Configure TCP/IP properties on NPS1 .....                                | 13 |
| Join NPS1 to the contoso.com domain.....                                 | 13 |
| User Account Control.....  | 14 |
| Install the NPS and DHCP server roles .....                              | 14 |
| Install the Group Policy Management feature .....                        | 15 |
| Configure NPS as a NAP health policy server .....                        | 15 |
| Configure NAP with a wizard.....   | 16 |
| Configure SHVs.....  | 17 |
| Configure DHCP on NPS1.....  | 18 |
| Open the DHCP console .....  | 18 |
| Enable NAP settings for the scope.....                                   | 18 |
| Configure the default user class.....                                    | 18 |
| Configure the default NAP class .....                                    | 19 |
| Configure NAP client settings in Group Policy .....                      | 19 |
| Configure security filters for the NAP client settings GPO .....         | 20 |
| Configure CLIENT1 .....  | 21 |
| Install Windows Vista on CLIENT1 .....                                   | 21 |
| Configure TCP/IP on CLIENT1 .....  | 21 |
| Test network connectivity for CLIENT1 .....                              | 22 |

|  |    |
|--|----|
| Configure DC1 as a remediation server .....                      | 23 |
| Renew IP addressing on CLIENT1 .....                             | 23 |
| Join CLIENT1 to the Contoso.com domain .....                     | 24 |
| Add CLIENT1 to the NAP client computers security group .....     | 24 |
| Enable Run on the Start menu .....                               | 25 |
| Verify Group Policy settings.....                                | 25 |
| Verifying NAP functionality .....                                | 26 |
| Verification of NAP auto-remediation.....                        | 26 |
| Verification of health policy enforcement.....                   | 27 |
| Configure WSHV to require an antivirus application .....         | 27 |
| Release and renew the IP address on CLIENT1 .....                | 27 |
| View the client restriction state .....                          | 28 |
| Allow CLIENT1 to become compliant.....                           | 28 |
| See Also .....   | 28 |
| Appendix.....  | 29 |
| Set UAC behavior of the elevation prompt for administrators..... | 29 |
| Review NAP client events .....                                   | 29 |
| Review NAP server events .....                                   | 30 |

# Step-by-Step Guide: Demonstrate DHCP NAP Enforcement in a Test Lab

---

Network Access Protection (NAP) is a new technology introduced in Windows Vista® and Windows Server® 2008. (NAP can also be deployed on computers running Windows Server 2008 R2 and Windows 7). NAP includes client and server components that allow you to create and enforce health requirement policies that define the required software and system configurations for computers that connect to your network. NAP enforces health requirements by inspecting and assessing the health of client computers, limiting network access when client computers are deemed noncompliant, and remediating noncompliant client computers for unrestricted network access. NAP enforces health requirements on client computers that are attempting to connect to a network. NAP also provides ongoing health compliance enforcement while a compliant client computer is connected to a network.

In addition, NAP provides an application programming interface (API) set that allows non-Microsoft software vendors to integrate their solutions into the NAP framework.

NAP enforcement occurs at the moment when client computers attempt to access the network through network access servers, such as a VPN server running Routing and Remote Access, or when clients attempt to communicate with other network resources. The way that NAP is enforced depends on the enforcement method you choose.

NAP enforces health requirements for the following:

- Internet Protocol security (IPsec)-protected communications
- Institute of Electrical and Electronics Engineers (IEEE) 802.1X-authenticated connections
- Virtual private network (VPN) connections
- Dynamic Host Configuration Protocol (DHCP) configuration
- Terminal Services Gateway (TS Gateway)

The step-by-step instructions in this paper will show you how to deploy a NAP DHCP enforcement test lab so that you can better understand how DHCP enforcement works.

## In this guide

This paper contains an introduction to NAP and instructions for setting up a test lab and deploying NAP with the DHCP enforcement method using two server computers and one client computer. The test lab lets you create and enforce client health requirements using NAP and DHCP.

### Important

The following instructions are for configuring a test lab using the minimum number of computers. Individual computers are needed to separate the services provided on the network and to clearly show the desired functionality. This configuration is neither designed to reflect best practices nor does it reflect a desired or recommended

configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed only to work on a separate test lab network.

## Scenario overview

In this test lab, NAP enforcement for DHCP network access control is deployed with a server running Windows Server 2008 or Windows Server 2008 R2 that has DHCP and the Network Policy Server (NPS) service installed, and a client computer running Windows Vista or Windows 7 with the NAP agent service running and DHCP enforcement client component enabled. A computer running Windows Server® 2003 is also used in the test lab as a domain controller and DNS server. The test lab will demonstrate how NAP-capable client computers are provided network access based on their compliance with network health requirements.

## NAP enforcement processes

Several processes are required for NAP to function properly: policy validation, NAP enforcement and network restriction, remediation, and ongoing monitoring to ensure compliance.

### Policy validation

System health validators (SHVs) are used by NPS to analyze the health status of client computers. SHVs are incorporated into network policies that determine actions to be taken based on client health status, such as the granting of full network access or the restricting of network access. Health status is monitored by client-side NAP components called system health agents (SHAs). NAP uses SHAs and SHVs to monitor, enforce, and remediate client computer configurations.

Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) are included with the Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 operating systems, and enforce the following settings for NAP-capable computers:

- The client computer has firewall software installed and enabled.
- The client computer has antivirus software installed and running.
- The client computer has current antivirus updates installed.
- The client computer has antispyware software installed and running.
- The client computer has current antispyware updates installed.
- Microsoft Update Services is enabled on the client computer.

In addition, if NAP-capable client computers are running Windows Update Agent, NAP can verify that the most recent software security updates are installed based on one of four possible values that match security severity ratings from the Microsoft Security Response Center (MSRC).

This test lab will use the WSHA and WSHV to require that client computers have turned on Windows Firewall, and have an antivirus application installed.

## NAP enforcement and network restriction

NAP enforcement settings allow you to limit network access of noncompliant clients to a restricted network, to defer restriction to a later date, or to merely observe and log the health status of NAP-capable client computers. The following settings are available:

- **Allow full network access.** This is the default setting. Clients that match the policy conditions are deemed compliant with network health requirements, and are granted unrestricted access to the network if the connection request is authenticated and authorized. The health compliance status of NAP-capable client computers is logged.
- **Allow limited access.** Client computers that match the policy conditions are deemed noncompliant with network health requirements, and are placed on the restricted network.
- **Allow full network access for a limited time.** Clients that match the policy conditions are temporarily granted full network access. NAP enforcement is delayed until the specified date and time.

You will create two network policies in this test lab. A compliant policy will grant full network access to an intranet network segment. A noncompliant policy will demonstrate network restriction by issuing a TCP/IP configuration to the client computer that places it on a restricted network.

## Remediation

Noncompliant client computers that are placed on a restricted network might undergo remediation. Remediation is the process of updating a client computer so that it meets current health requirements. If additional resources are required for a noncompliant computer to update its health state, these resources must be provided on the restricted network. For example, a restricted network might contain a File Transfer Protocol (FTP) server that provides current virus signatures so that noncompliant client computers can update their outdated signatures.

You can use NAP settings in NPS network policies to configure automatic remediation so that NAP client components automatically attempt to update the client computer when it is noncompliant.

This test lab includes a demonstration of automatic remediation. The **Enable auto-remediation of client computers** setting will be enabled in the noncompliant network policy, which will cause Windows Firewall to be turned on without user intervention.

## Ongoing monitoring to ensure compliance

NAP can enforce health compliance on compliant client computers that are already connected to the network. This functionality is useful for ensuring that a network is protected on an ongoing basis as health policies and the health of client computers change. Client computers are monitored when their health state changes, and when they initiate requests for network resources. This test lab includes a demonstration of ongoing monitoring when the client's DHCP-issued address is renewed. The NAP client computer sends a statement of health (SoH) with the DHCP address request, and is granted full or restricted access based on its current health state.

## DHCP NAP enforcement overview

The test environment described in this guide includes a domain controller running Windows Server 2003, a member server running Windows Server 2008 or Windows Server 2008 R2, and a client computer running Windows Vista or Windows 7. The domain controller, member server, and the client computer compose a private intranet and are connected through a common hub or layer 2 switch. Private addresses are used throughout the test lab configuration. The private network ID 192.168.0.0/24 is used for the intranet. The domain controller is named DC1 and is the primary domain controller for the domain named Contoso.com. The member server is named NPS1 and is configured as a DHCP server and a network policy server. The client is named CLIENT1 and is configured for automatic addressing through DHCP. The following figure shows the configuration of the test environment.

[5e0f1224-af8b-4b2c-9e7f-339aead191d6](#)

## Hardware and software requirements

The following are required components of the test lab:

- The product disc for Windows Server 2008 or Windows Server 2008 R2.
- The product disc for Windows Vista Business, Windows Vista Enterprise, or Windows Vista Ultimate. You can also use the product discs for Windows 7 Home Premium, Windows 7 Professional, or Windows 7 Ultimate.
- The product disc for Windows Server 2003 with Service Pack 2 (SP2).
- One computer that meets the minimum hardware requirements for Windows Server 2003 with SP2.



### Note

This lab demonstrates NAP support for the Active Directory® directory service in Windows Server 2003. You can also make the domain controller in this lab run Windows Server 2008 or Windows Server 2008 R2..

- One computer that meets the minimum hardware requirements for Windows Server 2008 or Windows Server 2008 R2.
- One computer that meets the minimum hardware requirements for Windows Vista or Windows 7.
- An Ethernet hub or layer 2 switch.

## Steps for configuring the test lab

There are three overall stages required to set up this test lab, one stage for each computer.

1. Configure DC1.

DC1 is a server computer running the Windows Server 2003 Standard Edition operating system. DC1 is configured as a domain controller with Active Directory and the primary DNS server for the intranet subnet.

## 2. Configure NPS1.

NPS1 is a server computer running Windows Server 2008 or Windows Server 2008 R2. NPS1 is configured with the Network Policy Server (NPS) service, which functions as a NAP health policy server and a Remote Authentication Dial-in User Service (RADIUS) server. NPS1 will also be configured with the DHCP service and function as a NAP enforcement server.

## 3. Configure CLIENT1.

CLIENT1 is a client computer running Windows Vista or Windows 7. CLIENT1 will be configured as a DHCP client and a NAP client.



### **Note**

You must be logged on as a member of the Domain Admins group or a member of the Administrators group on each computer to complete the tasks described in this guide. If you cannot complete a task while you are logged on with an account that is a member of the Administrators group, try performing the task while you are logged on with an account that is a member of the Domain Admins group.

After the NAP components are configured, this guide will provide steps for a demonstration of NAP enforcement and auto-remediation. The following sections provide details about how to perform these tasks.

## **Configure DC1**

DC1 is a computer running Windows Server 2003 Standard Edition with SP2, which provides the following services:

- A domain controller for the Contoso.com Active Directory domain.
- A DNS server for the Contoso.com DNS domain.

DC1 configuration consists of the following steps:

- Install the operating system.
- Configure TCP/IP.
- Install Active Directory and DNS.
- Create a user account and group in Active Directory.
- Create a NAP client computer security group.

The following sections explain these steps in detail.

## **Install the operating system on DC1**

Install Windows Server 2003 Standard Edition with SP2 as a stand-alone server.

▶ **To install the operating system on DC1**

1. Start your computer using the Windows Server 2003 product disc.
2. When prompted for a computer name, type **DC1**.

## **Configure TCP/IP on DC1**

Configure the TCP/IP protocol with a static IP address of 192.168.0.1 and the subnet mask of 255.255.255.0.

▶ **To configure TCP/IP on DC1**

1. Click **Start**, click **Run**, and then type **ncpa.cpl**.
2. Right-click **Local Area Connection**, and then click **Properties**.
3. Click **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. Select **Use the following IP address**. Type **192.168.0.1** next to **IP address** and **255.255.255.0** next to **Subnet mask**.
5. Verify that **Preferred DNS server** is blank.
6. Click **OK**, click **Close**, and then close the **Network Connections** window.

## **Configure DC1 as a domain controller and DNS server**

DC1 will serve as the only domain controller and DNS server for the Contoso.com domain.

▶ **To configure DC1 as a domain controller and DNS server**

1. To start the Active Directory Installation Wizard, click **Start**, click **Run**, type **dcpromo**, and then press ENTER.
2. In the **Active Directory Installation Wizard** dialog box, click **Next**.
3. Operating system compatibility information is displayed. Click **Next** again.
4. Verify that **Domain controller for a new domain** is selected, and then click **Next**.
5. Verify that **Domain in a new forest** is selected, and then click **Next** twice.
6. On the **Install or Configure DNS** page, select **No, just install and configure DNS on this computer**, and then click **Next**.
7. Type **Contoso.com** next to **Full DNS name for new domain**, and then click **Next**.
8. Confirm that the **Domain NetBIOS name** shown is **CONTOSO**, and then click **Next**.
9. Accept the default **Database Folder and Log Folder** directories, and then click **Next**.
10. Accept the default folder location for **Shared System Volume**, and then click **Next**.
11. Verify that **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems** is selected, and then click **Next**.
12. Leave the **Restore Mode Password** and **Confirm Password** text boxes blank, and then

- click **Next**.
13. Review the summary information provided, and then click **Next**.
  14. Wait while the wizard completes configuration of Active Directory and DNS services, and then click **Finish**.
  15. When prompted to restart the computer, click **Restart Now**.
  16. After the computer is restarted, log in to the CONTOSO domain using the Administrator account.

## Create a user account in Active Directory

Next, create a user account in Active Directory. This account will be used when logging in to NPS1 and CLIENT1.

### To create a user account in Active Directory

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, double-click **Contoso.com**, right-click **Users**, point to **New**, and then click **User**.
3. In the **New Object - User** dialog box, next to **Full name**, type **User1 User**, and in **User logon name**, type **User1**.
4. Click **Next**.
5. In **Password**, type the password that you want to use for this account, and in **Confirm password**, type the password again.
6. Clear the **User must change password at next logon** check box, and select the **Password never expires** check box.
7. Click **Next**, and then click **Finish**.
8. Leave the Active Directory Users and Computers console open for the following procedure.

## Add user1 to the Domain Admins group

Next, add the newly created user to the Domain Admins group so this user can be used for all configuration activities.

### To add a user to the Domain Admins group

1. In the Active Directory Users and Computers console tree, click **Users**.
2. In the details pane, double-click **Domain Admins**.
3. In the **Domain Admins Properties** dialog box, click the **Members** tab, and then click **Add**.
4. Under **Enter the object names to select (examples)**, type **User1**, the user name that

- you created in the preceding procedure, and then click **OK** twice.
5. Leave the Active Directory Users and Computers console open for the following procedure.

## Create a security group for NAP client computers

Next, create a security group for use with Group Policy security filtering. This security group will be used to apply NAP client computer settings to only the computers you specify. CLIENT1 will be added to this security group after it is joined to the domain.

### To create a security group for NAP client computers

1. In the Active Directory Users and Computers console tree, right-click **contoso.com**, point to **New**, and then click **Group**.
2. In the **New Object - Group** dialog box, under **Group name**, type **NAP client computers**.
3. Under **Group scope**, choose **Global**, under **Group type**, choose **Security**, and then click **OK**.
4. Close the Active Directory Users and Computers console.

## Configure NPS1

For the test lab, NPS1 will be running Windows Server 2008 or Windows Server 2008 R2, and will host the NPS service, which provides RADIUS authentication, authorization, and accounting. NPS1 configuration consists of the following steps:

- Install the operating system.
- Configure TCP/IP.
- Join the computer to the domain.
- Install the NPS and DHCP server roles.
- Install the Group Policy Management feature.
- Configure NPS as a NAP health policy server.
- Configure DHCP.
- Configure NAP client settings in Group Policy.

## Install Windows Server 2008 or Windows Server 2008 R2

### To install Windows Server 2008 or Windows Server 2008 R2

1. Start your computer by using the Windows Server 2008 or Windows Server 2008 R2 product CD.
2. When prompted for the installation type, choose **Custom**.

3. Follow the instructions that appear on your screen to finish the installation.

## Configure TCP/IP properties on NPS1

### ▶ To configure TCP/IP properties on NPS1

1. Click **Server Manager**.
2. Under **Server Summary**, click **View Network Connections**.
3. In the **Network Connections** dialog box, right-click **Local Area Connection**, and then click **Properties**.
4. In the **Local Area Connection Properties** dialog box, clear the **Internet Protocol Version 6 (TCP/IPv6)** check box. This step will reduce the complexity of the lab, particularly for those who are not familiar with IPv6.
5. In the **Local Area Connection Properties** dialog box, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
6. Select **Use the following IP address**. In **IP address**, type **192.168.0.2**. In **Subnet mask**, type **255.255.255.0**.
7. Select **Use the following DNS server addresses**. In **Preferred DNS server**, type **192.168.0.1**.
8. Click **OK**, and then click **Close** to close the **Local Area Connection Properties** dialog box.
9. Close the **Network Connections** window.
10. Do not close the **Server Manager** window. It will be used in the next procedure.
11. Next, check network communication between NPS1 and DC1 by running the **ping** command from NPS1.
12. Click **Start**, click **Run**, in **Open** type **cmd**, and then press ENTER.
13. In the command window, type **ping DC1**.
14. Verify that the response reads "Reply from 192.168.0.1."
15. Close the command window.

## Join NPS1 to the contoso.com domain

### ▶ To join NPS1 to the contoso.com domain

1. In Server Manager, under **Server Summary**, click **Change System Properties**.
2. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
3. In the **Computer Name/Domain Changes** dialog box, under **Computer name**, type **NPS1**.
4. In the **Computer Name/Domain Changes** dialog box, under **Member of**, choose

- Domain**, and then under **Domain**, type **Contoso.com**.
5. Click **More**. Under **Primary DNS suffix of this computer**, type **Contoso.com**, and then click **OK** twice.
  6. When prompted for a user name and password, type **User1** and the password for the user account that you added to the Domain Admins group, and then click **OK**.
  7. When you see a dialog box that welcomes you to the Contoso.com domain, click **OK**.
  8. When you are prompted that you must restart the computer, click **OK**.
  9. On the **System Properties** dialog box, click **Close**.
  10. When you are prompted to restart the computer, click **Restart Now**.
  11. After the computer has been restarted, click **Switch User**, then click **Other User** and log on to the CONTOSO domain with the **User1** account you created.

## User Account Control

When you configure the Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 operating systems, you are required to click **Continue** in the **User Account Control (UAC)** dialog box for some tasks. Several of the configuration tasks to follow require UAC approval. When prompted, always click **Continue** to authorize these changes. Alternatively, see the [Appendix](#) of this guide for instructions about how to set UAC behavior of the elevation prompt for administrators.

## Install the NPS and DHCP server roles

Next, install the NPS and DHCP server roles on NPS1.

### To install the NPS and DHCP server roles

1. Click **Start**, and then click **Server Manager**.
2. Under **Roles Summary**, click **Add roles**, and then click **Next**.
3. On the **Select Server Roles** page, select the **DHCP Server** and **Network Policy and Access Services** check boxes, and then click **Next** twice.
4. On the **Select Role Services** page, select the **Network Policy Server** check box, and then click **Next** twice.
5. On the **Select Network Connection Bindings** page, verify that **192.168.0.2** is selected, and then click **Next**.
6. On the **Specify IPv4 DNS Server Settings** page, verify that **contoso.com** is listed under **Parent domain**.
7. Type **192.168.0.1** under **Preferred DNS server IP address**, and click **Validate**. Verify that the result returned is **Valid**, and then click **Next**.
8. On the **Specify WINS Server Settings** page, accept the default setting of **WINS is not required on this network**, and then click **Next**.

9. On the **Add or Edit DHCP Scopes** page, click **Add**.
10. In the **Add Scope** dialog box, type **NAP Scope** next to **Scope Name**. Next to **Starting IP Address**, type **192.168.0.3**, next to **Ending IP Address**, type **192.168.0.10**, and next to **Subnet Mask**, type **255.255.255.0**.
11. Select the **Activate this scope** check box, click **OK**, and then click **Next**.
12. On the **Configure DHCPv6 Stateless Mode** page, select **Disable DHCPv6 stateless mode for this server**, and then click **Next**.
13. On the **Authorize DHCP Server** page, select **Use current credentials**. Verify that **CONTOSO\user1** is displayed next to **Username**, and then click **Next**.
14. On the **Confirm Installation Selections** page, click **Install**.
15. Verify the installation was successful, and then click **Close**.
16. Leave Server Manager open for the following procedure.

## Install the Group Policy Management feature

Group Policy will be used to configure NAP client settings in the test lab. To access these settings, the Group Policy Management feature must be installed on a computer running Windows Server 2008.

### To install the NPS server role

1. In Server Manager, under **Features Summary**, click **Add Features**.
2. Select the **Group Policy Management** check box, click **Next**, and then click **Install**.
3. Verify the installation was successful, and then click **Close** to close the **Add Features Wizard** dialog box.
4. Close Server Manager.

## Configure NPS as a NAP health policy server

To serve as a NAP health policy server, NPS1 must validate the system health of clients against the configured network health requirements. For this test lab, configuration of NPS as a NAP health policy server is performed using the NAP configuration wizard. The NAP wizard helps you configure each NAP component to work with the NAP enforcement method you choose. These components are displayed in the NPS console tree, and include:

- **System Health Validators**. System health validators (SHVs) define configuration requirements for computers that attempt to connect to your network. For the test lab, WSHV will be configured to require only that Windows Firewall is enabled.
- **Health Policies**. Health policies define which SHVs are evaluated, and how they are used in the validation of the configuration of computers that attempt to connect to your network. Based on the results of SHV checks, health policies classify client health status. The two

health policies in this test lab correspond to a compliant health state and a noncompliant health state.

- **Network Policies.** Network policies use conditions, settings, and constraints to determine who can connect to the network. There must be a network policy that will be applied to computers that are compliant with the health requirements, and a network policy that will be applied to computers that are noncompliant. For this test lab, compliant client computers will be allowed unrestricted network access. Clients determined to be noncompliant with health requirements will have their access restricted through DHCP to specify a restricted subnet. Noncompliant clients will also be optionally updated to a compliant state and subsequently granted unrestricted network access.
- **Connection Request Policies.** Connection request policies are conditions and settings that validate requests for network access and govern where this validation is performed. In this test lab, a connection request policy is used that requires DHCP as the network access server for client authentication.
- **RADIUS Clients and Servers.** RADIUS clients are network access servers. If you specify a RADIUS client, then a corresponding RADIUS server entry is required on the RADIUS client device. Remote DHCP servers are configured as RADIUS clients on NPS. A remote DHCP server is not used in this test lab; therefore, it will not be necessary to configure RADIUS clients and servers.
- **Remediation Server Groups.** Remediation server groups allow you to specify servers that are made available to noncompliant NAP clients so that they can remediate their health state and become compliant with health requirements. If these servers are required, they are automatically available to computers on the restricted access subnet when you add them to remediation server groups. This test lab includes a demonstration of the use of a remediation server group to provide domain services to a client with restricted network access.

## Configure NAP with a wizard

The NAP configuration wizard helps you to set up NPS as a NAP health policy server. The wizard provides commonly used settings for each NAP enforcement method, and automatically creates customized NAP policies for use with your network design. You can access the NAP configuration wizard from the NPS console.

### ▶ To configure NPS using the NAP wizard

1. Click **Start**, click **Run**, type **nps.msc**, and then press ENTER.
2. In the Network Policy Server console tree, click **NPS (Local)**.
3. In the details pane, under **Standard Configuration**, click **Configure NAP**. The NAP configuration wizard will start. See the following example.  
[91a88efd-0af3-40b4-be70-b7824d9423ce](#)
4. On the **Select Network Connection Method for Use with NAP** page, under **Network connection method**, select **Dynamic Host Configuration Protocol (DHCP)**, and then

- click **Next**.
5. On the **Specify NAP Enforcement Servers Running DHCP** page, click **Next**. Because this NAP health policy server has DHCP installed locally, we do not need to add RADIUS clients.
  6. On the **Specify DHCP Scopes** page, click **Next**. The test lab will use only one DHCP scope; therefore, no scope conditions are required.
  7. On the **Configure User Groups and Machine Groups** page, click **Next**. You do not need to configure groups for this test lab.
  8. On the **Specify a NAP Remediation Server Group and URL**, click **Next**. Remediation servers will be configured later in this test lab.
  9. On the **Define NAP Health Policy** page, verify that **Windows Security Health Validator** and **Enable auto-remediation of client computers** check boxes are selected, and then click **Next**.
  10. On the **Completing NAP Enforcement Policy and RADIUS Client Configuration** page, click **Finish**.
  11. Leave the NPS console open for the following procedure.

## Configure SHVs

SHVs define configuration requirements for computers that attempt to connect to your network. For the test lab, the WSHV will be configured to require only that Windows Firewall is enabled. Use one of the following procedures, depending on whether you are running Windows Server 2008 or Windows Server 2008 R2.

### To configure SHVs in Windows Server 2008

1. In the Network Policy Server console tree, double-click **Network Access Protection**, and then click **System Health Validators**.
2. In the details pane, under **Name**, double-click **Windows Security Health Validator**.
3. In the **Windows Security Health Validator Properties** dialog box, click **Configure**.
4. Clear all check boxes except **A firewall is enabled for all network connections**. See the following example.  
[cf2c67e2-15ec-4bde-9664-4648cba747c6](#)
5. Click **OK** to close the **Windows Security Health Validator** dialog box, and then click **OK** to close the **Windows Security Health Validator Properties** dialog box.
6. Close the Network Policy Server console.

### To configure system health validators in Windows Server 2008 R2

1. In the Network Policy Server console tree, open **Network Access Protection/System Health Validators/Windows Security Health Validator/Settings**.

2. In the details pane, under **Name**, double-click **Default Configuration**.
3. In the **Windows Security Health Validator** dialog box, in the left pane, select **Windows 7/Windows Vista**, and then under **Choose policy settings for Windows Security Health Validator**, clear all the check boxes except for **A firewall is enabled for all network connections**.
4. Click **OK** to close the **Windows Security Health Validator** dialog box, and then close the Network Policy Server console.

## Configure DHCP on NPS1

NPS1 is the member server that will provide DHCP addressing. The DHCP service was partially configured during installation with Server Manager. We will configure scope options further for NAP.

### Open the DHCP console

#### To open the DHCP console

1. Click **Start**, click **Run**, type **dhcpcmgmt.msc**, and then press ENTER.
2. Leave this window open for all DHCP configuration tasks.

### Enable NAP settings for the scope

First, enable the default NAP profile for the NAP scope.

#### To enable the default NAP profile

1. In the DHCP console, double-click **nps1.contoso.com**, and then double-click **IPv4**.
2. Right-click **Scope [192.168.0.0] NAP Scope**, and then click **Properties**.
3. On the **Network Access Protection** tab, under **Network Access Protection Settings**, choose **Enable for this scope**, verify that **Use default Network Access Protection profile** is chosen, and then click **OK**.

### Configure the default user class

Next, configure scope options for the default user class. These server options are used when a compliant client computer attempts to access the network and obtain an IP address from the DHCP server.

#### To configure default user class scope options

1. In the DHCP console tree, under **Scope [192.168.0.0] NAP Scope**, right-click **Scope Options**, and then click **Configure Options**.
2. On the **Advanced** tab, verify that **Default User Class** is chosen next to **User class**.

3. Select the **006 DNS Servers** check box, in **IP Address**, under **Data entry**, type **192.168.0.1**, and then click **Add**.
4. Select the **015 DNS Domain Name** check box, in **String value**, under **Data entry**, type **contoso.com**, and then click **OK**. The contoso.com domain is a full-access network assigned to compliant NAP clients.

 **Note**

The **003 Router** option is configured in the default user class if a default gateway is required for client computers. Because all computers in the test lab are located on the same subnet, this option is not required.

## Configure the default NAP class

Next, configure scope options for the default network access protection class. These server options are used when a noncompliant client computer attempts to access the network and obtain an IP address from the DHCP server.

### To configure default NAP class scope options

1. In the DHCP console tree, under **Scope [192.168.0.0] NAP Scope**, right-click **Scope Options**, and then click **Configure Options**.
2. On the **Advanced** tab, next to **User class**, choose **Default Network Access Protection Class**.
3. Select the **006 DNS Servers** check box, in **IP Address**, under **Data entry**, type **192.168.0.1**, and then click **Add**.
4. Select the **015 DNS Domain Name** check box, in **String value**, under **Data entry**, type **restricted.contoso.com**, and then click **OK**. The restricted.contoso.com domain is a restricted-access network assigned to noncompliant NAP clients.

 **Note**

The **003 Router** option is configured in the default NAP class if a default gateway is required for client computers to reach the DHCP server or remediation servers on a different subnet. Because all computers in the test lab are located on the same subnet, this option is not required.

## Configure NAP client settings in Group Policy

The following NAP client settings will be configured in a new Group Policy object (GPO) using the Group Policy Management feature on NPS1:

- NAP enforcement clients
- NAP Agent service
- Security Center user interface

After these settings are configured in the GPO, security filters will be added to enforce the settings on computers you specify. The following section describes these steps in detail.

### ▶ To configure NAP client settings in Group Policy

1. On NPS1, click **Start**, click **Run**, type **gpme.msc**, and then press ENTER.
2. In the **Browse for a Group Policy Object** dialog box, next to **Contoso.com**, click the icon to create a new GPO, type **NAP client settings** for the name of the new GPO, and then click **OK**.
3. The Group Policy Management Editor window will open. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\System Services**.
4. In the details pane, double-click **Network Access Protection Agent**.
5. In the **Network Access Protection Agent Properties** dialog box, select the **Define this policy setting** check box, choose **Automatic**, and then click **OK**.
6. In the console tree, open **Network Access Protection\NAP Client Configuration\Enforcement Clients**.
7. In the details pane, right-click **DHCP Quarantine Enforcement Client**, and then click **Enable**.
8. In the console tree, right-click **NAP Client Configuration**, and then click **Apply**.

#### **Note**

If you are running Windows Server 2008 R2, you can skip this step.

9. In the console tree, navigate to **Computer Configuration\Policies\Administrative Templates\Windows Components\Security Center**.
10. In the details pane, double-click **Turn on Security Center (Domain PCs only)**, choose **Enabled**, and then click **OK**.
11. Close the **Group Policy Management Editor** window.
12. If you are prompted to apply settings, click **Yes**.

### Configure security filters for the NAP client settings GPO

Next, configure security filters for the NAP client settings GPO. This prevents NAP client settings from being applied to server computers in the domain.

### ▶ To configure security filters for the NAP client settings GPO

1. On NPS1, click **Start**, click **Run**, type **gpmc.msc**, and then press ENTER.
2. In the Group Policy Management Console (GPMC) tree, navigate to **Forest: Contoso.com\Domains\Contoso.com\Group Policy Objects\NAP client settings**.
3. In the details pane, under **Security Filtering**, click **Authenticated Users**, and then click **Remove**.
4. When you are prompted to confirm the removal of delegation privilege, click **OK**.

5. In the details pane, under **Security Filtering**, click **Add**.
6. In the **Select User, Computer, or Group** dialog box, under **Enter the object name to select (examples)**, type **NAP client computers**, and then click **OK**.
7. Close the GPMC.



#### Note

CLIENT1 will be added to the NAP client computers security group after it is joined to the domain.

## Configure CLIENT1

CLIENT1 is a computer running Windows Vista or Windows 7 that you will use to demonstrate how NAP can be used with DHCP to help protect a network from noncompliant client computers. CLIENT1 configuration is performed in the following steps:

- Install the operating system.
- Configure TCP/IP.
- Verify network connectivity.
- Join the computer to the domain.
- Add CLIENT1 to the NAP client computers security group and restart the computer.
- Enable **Run** on the **Start** menu.
- Verify Group Policy settings.

The following sections explain these steps in detail.

### Install Windows Vista on CLIENT1

#### ▶ To install the operating system on CLIENT1

1. Start your computer using the product discs for Windows Vista or Windows 7.
2. When prompted for the installation type, choose **Custom Installation**.
3. When prompted for a computer name, type **CLIENT1**.
4. On the **Select your computer's current location** page, click **Work**.
5. Follow the rest of the instructions that appear on your screen to finish the installation.

### Configure TCP/IP on CLIENT1

#### ▶ To configure TCP/IP on CLIENT1

1. Click **Start**, click **Run**, and then type **ncpa.cpl**.



#### Important

You must enable the **Run** command to complete this step. For more

information about how to enable the **Run** command, see [To enable Run on the Start menu](#) procedure later in this document.

2. Right-click **Local Area Connection**, and then click **Properties**.
3. In the **Local Area Connection Properties** dialog box, clear the **Internet Protocol Version 6 (TCP/IPv6)** check box. This will reduce the complexity of the lab, particularly for those who are not familiar with IPv6.
4. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
5. Verify that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
6. Click **OK**, and then click **Close** to close the **Local Area Connection Properties** dialog box.
7. Close the **Network Connections** and **Network and Sharing Center** windows.

## Test network connectivity for CLIENT1

Because CLIENT1 has not joined the domain, it has not yet received Group Policy settings to start the NAP Agent service. When the NAP Agent service is not running, CLIENT1 is evaluated as non-NAP-capable. By default, the NAP configuration wizard provides restricted access to non-NAP-capable clients. Run the **ping** command from CLIENT1 to confirm the loss of network communication between CLIENT1 and DC1.

### ▶ To use the ping command to check network connectivity

1. Click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
2. In the command window, type **ping 192.168.0.1**, and then press ENTER.
3. Verify that the response reads "PING: transmit failed."
4. In the command window, type **ipconfig**, and then press ENTER.
5. In the command output, verify that the value of **Connection-specific DNS Suffix** is **restricted.contoso.com** and that the value of **Subnet Mask** is **255.255.255.255**. CLIENT1 is configured with a classless network address, causing its network access to be restricted.
6. In the command window, type **route print -4**, and then press ENTER.
7. In the command output, below **Active Routes**, verify that a **Network Destination** of **192.168.0.1** is not displayed. Because CLIENT1 has a classless network address and no active route to contact DC1, it does not have access to domain services.
8. In the command output, below **Active Routes**, verify that a **Network Destination** of **192.168.0.2** is displayed. This is the IP address of NPS1, which serves as the NAP DHCP enforcement server for the test lab. The NAP DHCP enforcement server is automatically available to clients on the restricted network. You do not have to add this server to a remediation server group.

9. Leave the command window open for the following procedure.

## Configure DC1 as a remediation server

Next, configure DC1 as a remediation server so that CLIENT1 has access to DNS and Active Directory when it is granted restricted access.

### ▶ To configure DC1 as a remediation server

1. On NPS1, click **Start**, click **Run**, type **nps.msc**, and then press ENTER.
2. In the Network Policy Server console tree, open **Policies**, and then click **Network Policies**.
3. In the details pane, double-click **NAP DHCP Non NAP-Capable**.
4. On the **Settings** tab, under **Network Access Protection**, click **NAP Enforcement**.
5. Under **Remediation Server Group and Troubleshooting URL**, click **Configure**.
6. In the **Remediation Servers and Troubleshooting URL** dialog box, under **Remediation Server Group**, click **New Group**.
7. In the **New Remediation Server Group** dialog box, under **Group Name**, type **Domain services**, and then click **Add**.
8. In the **Add New Server** dialog box, under **Friendly name**, type **DC1**. Under **IP address or DNS name**, type **192.168.0.1**, and then click **OK** twice.
9. Verify that the new remediation server group is selected under **Remediation Server Group**, and then click **OK** to close the **Remediation Servers and Troubleshooting URL** dialog box.
10. Click **OK** to close the **NAP DHCP Non NAP-Capable Properties** window.
11. In the details pane, double-click **NAP DHCP Noncompliant**.
12. Click the **Settings** tab, click **NAP Enforcement**, and then, under **Remediation Server Group and Troubleshooting URL**, click **Configure**. From the list under **Remediation Server Group**, select **Domain services**, and then click **OK** twice. DC1 has now been enabled as a remediation server for non-NAP-capable and noncompliant computers.
13. Leave the Network Policy Server console open for the following procedure.

## Renew IP addressing on CLIENT1

Next, obtain a new IP address profile for CLIENT1 from DHCP.

### ▶ To renew IP addressing on CLIENT1

1. On CLIENT1, in the **Administrator: Command Prompt** window, type **ipconfig /renew**, and then press ENTER.
2. In the command window, type **ping 192.168.0.1**, and then press ENTER.

3. Verify that the response reads "Reply from 192.168.0.1."
4. In the command window, type **ipconfig**, and then press ENTER.
5. In the command output, verify that the value of **Connection-specific DNS Suffix** is **restricted.contoso.com** and that the value of **Subnet Mask** is **255.255.255.255**. Because the NAP Agent service is not running on CLIENT1, restricted access to the network is still enforced.
6. In the command window, type **route print -4**, and then press ENTER.
7. In the command output, below **Active Routes**, verify that a **Network Destination** of **192.168.0.1** is displayed. Because DC1 is a member of the remediation servers group, CLIENT1 has been granted access to domain services on the restricted network.
8. Close the command window.

## Join CLIENT1 to the Contoso.com domain

Because CLIENT1 now has access to domain services, it can be joined to the domain.

### To join CLIENT1 to the Contoso.com domain

1. Click **Start**, right-click **Computer**, and then click **Properties**.
2. Under **Computer name, domain, and workgroup settings**, click **Change settings**.
3. In the **System Properties** dialog box, click **Change**.
4. In the **Computer Name/Domain Changes** dialog box, select **Domain**, and then type **Contoso.com**.
5. Click **More**, and in **Primary DNS suffix of this computer**, type **Contoso.com**.
6. Click **OK** twice.
7. When prompted for a user name and password, type the user name and password for the User1 account, and then click **OK**.
8. When you see a dialog box that welcomes you to the Contoso.com domain, click **OK**.
9. When you see a dialog box that tells you that you must restart the computer to apply changes, click **OK**.
10. In the **System Properties** dialog box, click **Close**.
11. In the dialog box that prompts you to restart the computer, click **Restart Later**.



#### Note

Before you restart the computer, you must add it to the NAP client computers security group so that CLIENT1 will receive NAP client settings from Group Policy.

## Add CLIENT1 to the NAP client computers security group

After joining the domain, CLIENT1 must be added to the NAP client computers security group so that it can receive NAP client settings.

### ▶ To add CLIENT1 to the NAP client computers security group

1. On DC1, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, click **Contoso.com**.
3. In the details pane, double-click **NAP client computers**.
4. In the **NAP client computers Properties** dialog box, click the **Members** tab, and then click **Add**.
5. In the **Select Users, Contacts, Computers, or Groups** dialog box, click **Object Types**, select the **Computers** check box, and then click **OK**.
6. Under **Enter the object names to select (examples)**, type **CLIENT1**, and then click **OK**.
7. Verify that **CLIENT1** is displayed below **Members**, and then click **OK**.
8. Close the Active Directory Users and Computers console.
9. Restart CLIENT1 to apply the new security group membership.

## Enable Run on the Start menu

The **run** command is useful for several procedures in the test lab. To make it readily available, we will enable **Run** on the **Start** menu.

### ▶ To enable Run on the Start menu

1. After CLIENT1 has been restarted, click **Switch User**, click **Other User** and then log on to the CONTOSO domain with the **User1** account you created.
2. Right-click **Start**, and then click **Properties**.
3. In the **Taskbar and Start Menu Properties** window, select **Start menu**, and then click **Customize**.
4. In the **Customize Start Menu** window, select the **Run command** check box, and then click **OK** twice.

## Verify Group Policy settings

After it has been restarted, CLIENT1 will receive Group Policy settings to enable the NAP Agent service and DHCP enforcement client. The command line will be used to verify these settings.

### ▶ To verify Group Policy settings on CLIENT1

1. Click **Start**, click **Run**, type **cmd**, and then press ENTER.
2. In the command window, type **netsh nap client show grouppolicy**, and then press ENTER.
3. In the command output, under **Enforcement clients**, verify that the **Admin** status of the

#### **DHCP Quarantine Enforcement Client is Enabled.**

4. In the command window, type **netsh nap client show state**, and then press ENTER.
5. In the command output, under **Enforcement client state**, verify that the **Initialized** status of the **DHCP Quarantine Enforcement Client** is **Yes**.
6. Close the command window.

## **Verifying NAP functionality**

The following procedures are used to verify that the NAP infrastructure is functioning correctly:

- Verification of NAP auto-remediation. CLIENT1 is automatically remediated when Windows Firewall is turned off, causing Windows Firewall to be turned back on.
- Verification of NAP policy enforcement. NAP policy is revised to be more restrictive, causing CLIENT1 to be noncompliant with policy and unable to remediate itself. When CLIENT1 is in a noncompliant state, its network access will be restricted.

### **Verification of NAP auto-remediation**

The NAP DHCP noncompliant network policy specifies that noncompliant computers should be automatically remediated. Use the following procedure to verify that CLIENT1 is automatically remediated to a compliant state when Windows Firewall is turned off.

#### **▶ To verify that CLIENT1 is remediated automatically when Windows Firewall is turned off**

1. On CLIENT1, click **Start**, and then click **Control Panel**.
2. Click **Security**, click **Security Center**, and then click **Windows Firewall**.
3. In the **Windows Firewall** dialog box, click **Change settings**.
4. In the **Windows Firewall Settings** dialog box, click **Off (not recommended)**, and then click **OK**.
5. In Windows Security Center, you will see that the status of Windows Firewall is displayed as **Off** and is then displayed as **On**.
6. You might see a message in the notification area that indicates the computer does not meet health requirements. This message is displayed because Windows Firewall has been turned off. Click this message for more information about the health status of CLIENT1. See the following example.  
[6a91f72c-b24f-42a9-8619-666a48dac69a](#)
7. The NAP client will automatically turn Windows Firewall on to become compliant with network health requirements. The following message will appear in the notification area:  
**This computer meets the requirements of this network.** See the following example.  
[738a6c72-9e64-42e6-8c9d-fa276bd1056f](#)

Because auto-remediation occurs rapidly, you might not see one or both of these

messages.

## Verification of health policy enforcement

Network health policy enforcement will be verified by configuring an additional requirement in network policy that is not met by CLIENT1, and demonstrating that CLIENT1 is subsequently placed on the restricted network.

### Configure WSHV to require an antivirus application

Configure NPS1 so that antivirus software is a requirement for system health. Because no antivirus program is installed on CLIENT1 and the NAP client components cannot remediate its health, CLIENT1 will be noncompliant.

#### ▶ To configure the system health validator policy to require antivirus software

1. On NPS1, in the Network Policy Server console, open **NPS (Local)**, then **Network Access Protection**, then **System Health Validators**.
2. Under **Name**, double-click **Windows Security Health Validator**.
3. In the **Windows Security Health Validator Properties** dialog box, click **Configure**.
4. In the **Windows Security Health Validator** dialog box, under **Virus Protection**, select the **An antivirus application is on** check box.
5. Click **OK**, and then click **OK** again to close the **Windows Security Health Validator Properties** window.

### Release and renew the IP address on CLIENT1

To reevaluate the health state of CLIENT1 against the new network health requirements, turn Windows Firewall off. CLIENT1 will automatically remediate the Windows Firewall setting, but because an antivirus program is not installed, the health requirement for an antivirus program cannot be met. Therefore, CLIENT1 will remain in a noncompliant state and will obtain an IP address configuration for the restricted network.

#### ▶ To release and then renew the IP address on CLIENT1

1. On CLIENT1, in the **Windows Firewall** dialog box, click **Change settings**.
2. In the **Windows Firewall Settings** dialog box, click **Off (not recommended)**, and then click **OK**.
3. In Windows Security Center, you will see that Windows Firewall is initially displayed as off, and then displayed as on. Although Windows Firewall is turned on, CLIENT1 cannot install an antivirus application automatically, so it will remain in a noncompliant state and its network access will be restricted.

## View the client restriction state

Because the client computer is in a noncompliant state, the DHCP server will assign an IP address to the client computer for the restricted network. You can tell that the client is on the restricted network because the DHCP server assigns a connection-specific DNS suffix of `restricted.contoso.com`. The following figure shows an example.

[dfe2e27b-da4a-4a77-9dea-fdd439f97d82](#)

You might see a message in the notification area that indicates the computer does not meet the corporate security requirements.

## View the client's restriction state with Netsh

You can also check the restriction state of the computer using a NAP Netsh command.

### ▶ To use a Netsh command to show the NAP client's health state

1. On CLIENT1, at the command prompt, type **netsh nap client show state**, and then press ENTER.
2. Scroll up the command window to display the **Client state** section. The **Restriction state** should be "Restricted."

## Allow CLIENT1 to become compliant

Next, configure NPS1 to remove the antivirus health requirement so that CLIENT1 can be compliant. You can use **ipconfig** to release and renew the IP address on CLIENT1 to generate a new SoH.

### ▶ To configure NPS1 health requirements to allow CLIENT1 to become compliant

1. On NPS1, open the Network Policy Server console.
2. Double-click **Windows Security Health Validator**.
3. In the **Windows Security Health Validator Properties** dialog box, click **Configure**.
4. In the **Windows Security Health Validator** dialog box, under **Virus Protection**, clear the **An antivirus application is on** check box.
5. Click **OK** twice to complete configuration of the WSHV.
6. On CLIENT1, type **ipconfig /release**, and then type **ipconfig /renew** at the elevated command prompt to obtain a new IP address configuration with unrestricted access.
7. Verify that new IP address configuration is assigned the connection-specific DNS suffix of **contoso.com**.

## See Also

<http://go.microsoft.com/fwlink/?LinkId=56443>

# Appendix

---

This appendix will help you with troubleshooting techniques and the setting of optional features in Windows Server 2008 or Windows Server 2008 R2 and Windows Vista or Windows 7.

## Set UAC behavior of the elevation prompt for administrators

By default, User Account Control (UAC) is enabled in Windows Server 2008 or Windows Server 2008 R2 and Windows Vista or Windows 7. This service will prompt for permission to continue during several of the configuration tasks described in this guide. In all cases, you can click **Continue** in the UAC dialog box to grant this permission, or you can use the following procedure to change the UAC behavior of the elevation prompt for administrators.

### ▶ To set UAC behavior of the elevation prompt for administrators

1. Click **Start**, point to **All Programs**, click **Accessories**, and then click **Run**.
2. Type **secpol.msc**, and press ENTER.
3. In the **User Account Control** dialog box, click **Continue**.
4. In the left pane, double-click **Local Policies**, and then click **Security Options**.
5. In the right pane, double-click **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode**.
6. From the drop-down list box, choose **Elevate without prompting**, and then click **OK**.
7. Close the **Local Security Policy** window.

## Review NAP client events

Reviewing information contained in NAP client events can assist you with troubleshooting. It can also help you to understand NAP client functionality.

### ▶ To review NAP client events in Event Viewer

1. Click **Start**, point to **All Programs**, click **Accessories**, and then click **Run**.
2. Type **eventvwr.msc**, and press ENTER.
3. In the left tree, navigate to **Event Viewer(Local)\Applications and Services Logs\Microsoft\Windows\Network Access Protection\Operational**.
4. Click an event in the middle pane.
5. By default, the **General** tab is displayed. Click the **Details** tab to view additional information.
6. You can also right-click an event and then click **Event Properties** to open a new window for reviewing events.

## Review NAP server events

Reviewing information contained in Windows System events on your NAP servers can assist you with troubleshooting. It can also help you to understand NAP server functionality.

### To review NAP server events in Event Viewer

1. Click **Start** and then click **Run**.
2. Type **eventvwr.msc**, and press ENTER.
3. In the left tree, navigate to **Event Viewer(Local)\Custom Views\Server Roles\Network Policy and Access Services**.
4. Click an event in the middle pane.
5. By default, the **General** tab is displayed. Click the **Details** tab to view additional information.
6. You can also right-click an event and then click **Event Properties** to open a new window for reviewing events.