





Test Lab Guide: Demonstrate Forefront UAG DirectAccess with Network Access Protection (NAP)

Microsoft Corporation  
Published: July 2010

Abstract

DirectAccess is a new feature in the Windows® 7 and Windows Server® 2008 R2 operating systems that enables remote users to securely access intranet shared folders, Web sites, and applications without connecting to a virtual private network (VPN). Forefront Unified Access Gateway (UAG) 2010 extends the DirectAccess Windows DirectAccess value by adding support for highly available DirectAccess arrays and integrated support for IPv4 intranet resources. Network Access Protection (NAP) monitors and assesses the health of client computers when they attempt to connect or communicate on a network. NAP with DirectAccess allows you to specify that only DirectAccess clients that meet system health requirements can reach intranet resources. This paper contains step-by-step instructions for extending the [Test Lab Guide: Demonstrate UAG DirectAccess](http://go.microsoft.com/fwlink/?LinkID=198436) to demonstrate UAG DirectAccess with NAP on a simulated Internet, intranet, and home network.



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.

© 2010 Microsoft Corporation. All rights reserved.

Last Updated July 26, 2010

Microsoft, Windows, Active Directory, Internet Explorer, 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

[Introduction 1](#_Toc268075606)

[In this guide 1](#_Toc268075607)

[Overview of the test lab scenario 2](#_Toc268075608)

[Configuration component requirements 3](#_Toc268075609)

[Steps for configuring the test lab 4](#_Toc268075610)

[STEP 1: Complete the Demonstrate UAG DirectAccess Test Lab Guide 6](#_Toc268075611)

[STEP 2: Install Update 1 on UAG1 6](#_Toc268075612)

[STEP 3: Install the CA Server Role on APP1 6](#_Toc268075613)

[STEP 4: Configure the Subordinate CA and CA Permissions on APP1 7](#_Toc268075614)

[STEP 5: Install the NPS and HRA Server Roles on DC1 8](#_Toc268075615)

[STEP 6: Configure the NAP Health Policy Server on DC1 8](#_Toc268075616)

[STEP 7: Reconfigure the DirectAccess Settings on UAG1 9](#_Toc268075617)

[STEP 8: Configure NAP Client Settings in Group Policy 10](#_Toc268075618)

[STEP 9: Verify NAP Health Evaluation for CLIENT1 11](#_Toc268075619)

[STEP 10: Verify NAP Autoremediation Functionality for CLIENT1 12](#_Toc268075620)

[STEP 11: Demonstrate NAP Functionality for CLIENT1 When Connected to HomeNet 13](#_Toc268075621)

[STEP 12: Verify CLIENT1 Cannot Connect to Intranet Resources when it is Non-Compliant 14](#_Toc268075622)

[STEP 13: Snapshot the Configuration 15](#_Toc268075623)

[Additional Resources 15](#_Toc268075624)

# Introduction

DirectAccess is a new feature in the Windows 7 and Windows Server 2008 R2 operating systems that gives users the experience of being seamlessly connected to their intranet any time they have Internet access. With DirectAccess enabled, requests for intranet resources (such as e-mail servers, shared folders, or intranet Web sites) are securely directed to the intranet, without requiring users to connect to a VPN. DirectAccess provides increased productivity for a mobile workforce by offering the same connectivity experience both inside and outside the office.

Forefront Unified Access Gateway (UAG) extends the value of the Windows DirectAccess solution by adding features that meet the requirements of many enterprise deployments:

* Support for arrays of up to 8 UAG DirectAccess servers where configuration is done once on an array master and is automatically deployed to all other members of the array
* Support for Network Load Balancing, which enables the UAG DirectAccess array to be highly available without requiring the use of an external hardware load balancer
* Support for IPv4-only networks, network segments, or server or application resources with the help of NAT64/DNS64 IPv6/IPv4 transition technologies.

Network Access Protection (NAP), built into Windows Server 2008 R2 and Windows 7, enforces health requirements by monitoring and assessing the health of client computers when they attempt to connect or communicate on a network. Client computers that are not in compliance with system health requirements can be provided with restricted network access until their configuration is updated and brought into compliance.

The combination of DirectAccess with NAP allows you to verify that DirectAccess client computers meet your system health requirements before allowing access to the intranet.

To learn more about UAG DirectAccess, see the following resources:

* [Forefront UAG DirectAccess Design Guide](http://technet.microsoft.com/en-us/library/ee406191.aspx)
* [Forefront UAG DirectAccess Deployment Guide](http://technet.microsoft.com/en-us/library/dd857320.aspx)

To learn more about NAP, see the [Network Access Protection Product Information Web site](http://www.microsoft.com/windowsserver2008/en/us/nap-main.aspx).

## In this guide

This guide provides step-by-step instructions for configuring UAG DirectAccess with NAP in a test lab so that you can see how it works. You will set up and deploy Forefront UAG DirectAccess using five server computers, two client computers, Windows Server 2008 R2 Enterprise edition, and Windows 7 Ultimate Edition. The Test Lab simulates intranet, Internet, and a home networks, and demonstrates Forefront UAG DirectAccess in different Internet connection scenarios. The starting point for this paper is the [Test Lab Guide: Demonstrate UAG DirectAccess](http://go.microsoft.com/fwlink/?LinkID=198436).

|  |
| --- |
| **ImportantImportant:** |
| These instructions are designed 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 show clearly the required functionality. This configuration is not designed to reflect best practices, nor does it reflect a required or recommended configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed to work only on a separate test lab network. For more information on planning and deploying DirectAccess with Forefront UAG, please see the [Forefront UAG DirectAccess design guide](http://technet.microsoft.com/en-us/library/ee406191.aspx) and the [Forefront UAG DirectAccess deployment guide](http://technet.microsoft.com/en-us/library/dd857320.aspx) |

# Overview of the test lab scenario

In this test lab scenario, Forefront UAG DirectAccess is deployed with:

* One computer running Windows Server 2008 R2 Enterprise Edition (DC1), that is configured as an intranet domain controller, Domain Name System (DNS) server, Dynamic Host Configuration Protocol (DHCP) server, and an enterprise root certification authority (CA).
* One intranet member server running Windows Server 2008 R2 Enterprise Edition (UAG1), that is configured as the first Forefront UAG DirectAccess server in a Forefront UAG DirectAccess server array.
* One intranet member server running Windows Server 2008 R2 Enterprise Edition (APP1) that is configured as a general application server and network location server. This server is used to complete a Forefront UAG DirectAccess server array to highlight centralized configuration and Network Load Balancing high availability.
* One intranet member server running Windows Server 2003 SP2 (APP3) that is configured as an IPv4 only web and file server. This server is used to highlight the NAT64/DNS64 capabilities.
* One standalone server running Windows Server 2008 R2 Enterprise Edition (INET1) that is configured as an Internet DNS and DHCP server.
* One standalone client computer running Windows 7 Ultimate Edition (NAT1), that is configured as a network address translator (NAT) device using Internet Connection Sharing.
* One roaming member client computer running Windows 7 Ultimate Edition (CLIENT1) that is configured as a DirectAccess client.

The test lab consists of three subnets that simulate the following:

* A home network named Homenet (192.168.137.0/24) connected to the Internet by a NAT.
* The Internet (131.107.0.0/24).
* An intranet named Corpnet (10.0.0.0/24) separated from the Internet by the Forefront UAG DirectAccess server.

Computers on each subnet connect using either a physical or virtual hub or switch, as shown in the following figure.



# Configuration component requirements

The following components are required for configuring Forefront UAG DirectAccess in the test lab:

* The product disc or files for Windows Server 2008 R2 Enterprise Edition.
* The product disc or files for Windows Server 2003 Enterprise SP2
* The product disc or files for of Windows 7 Ultimate.
* Five computers or virtual machines that meet the minimum hardware requirements for Windows Server 2008 R2 Enterprise; two of these computers has two network adapters installed.
* One computer or virtual machine that meets the minimum hardware requirements for Windows Server 2003 SP2
* Two computers or virtual machines that meet the minimum hardware requirements for Windows 7 Ultimate; one of these computers has two network adapters installed.
* The product disc or a downloaded version of Microsoft Forefront Unified Access Gateway (UAG) RTM.

This Test Lab Guide demonstrates UAG DirectAccess with NAP in full enforcement mode where the UAG DirectAccess server requires health certificates for authentication to access resources through the intranet tunnel. Noncompliant UAG DirectAccess clients cannot access the intranet and cannot use their computer certificate for authentication.

For more information about the different modes of NAP, see [Stages of a NAP Deployment](http://technet.microsoft.com/en-us/library/dd125311(WS.10).aspx).

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. It is important to remember that 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.

Attempting to adapt this test lab configuration to a pilot or production deployment can result in configuration or functionality issues. To ensure proper configuration and operation of UAG DirectAccess with NAP for your pilot or production DirectAccess deployment, use the information in [Planning Forefront UAG DirectAccess with Network Access Protection (NAP)](http://technet.microsoft.com/en-us/library/ee809068.aspx) for your planning and design decisions and [Forefront UAG DirectAccess Deployment Guide](http://technet.microsoft.com/en-us/library/dd857320.aspx) for the steps to configure the UAG DirectAccess server and supporting infrastructure servers.

# Steps for configuring the test lab

The following sections describe how to configure UAG1, APP1 and DC1 for DirectAccess with NAP. After UAG1, APP1 and DC1 are configured, this guide provides steps for demonstrating NAP functionality for CLIENT1 when it is connected to the Corpnet and Internet subnets.

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. For all tasks described in this document you can use the **CONTOSO\User1** account created when you went through the steps in the UAG DirectAccess [Test Lab Guide: Demonstrate UAG DirectAccess](http://go.microsoft.com/fwlink/?LinkID=198436).

The following procedures are performed to enable and allow you to test each of them:

* **Step 1: Complete the Demonstrate UAG DirectAccess Test Lab Guide –** The first step is to complete all the steps in the [Test Lab Guide: Demonstrate UAG DirectAccess](http://go.microsoft.com/fwlink/?LinkID=198436).
* **STEP 2: Install UAG Update 1 on UAG1**. You will install UAG Update 1 to bring UAG up to date for full NAP enforcement functionality.
* **STEP 3: Install the CA Server Role on APP1**. In this step you will install a subordinate Certification Authority on APP1 so that it will be able to create health certificates for DirectAccess NAP clients.
* **STEP 4: Configure the Subordinate CA and CA Permissions on APP1**. In this step you will configure the subordinate CA on APP1 so that it will automatically grant certificates when requested by the DC1. You will also configure permissions on the CA to enable DC1 to issue and manage certificate, manage the CA and request certificates.
* **STEP 5: Install the NPS and HRA Server Roles on DC1**. In this step you will install the Network Policy Server and Health Registration Authority Server roles on DC1.
* **STEP 6: Configure the NAP Health Policy Server on DC1**. In this step you will configure the IPsec with HRA enforcement and enable Autoremediation for DirectAccess NAP clients. You will also configure the Windows Security Health Validator to require a firewall to be enabled for all network connections.
* **STEP 7: Reconfigure the DirectAccess Settings on UAG1**. In this step you will reconfigure the DirectAccess settings on UAG1 to support NAP policy enforcement for DirectAccess clients.
* **STEP 8: Configure NAP Client Settings in Group Policy on DC1**. In this step you will configure a number of Group Policy settings in the DirectAccess clients GPO that are required Network Access Protection clients.
* **STEP 9: Verify NAP Health Evaluation for CLIENT1**. In this step you will confirm that CLIENT1 was received the Group Policy settings required for NAP clients and confirm that CLIENT1 received a certificate of health from DC1.
* **STEP 10: Verify NAP Autoremediation Functionality for CLIENT1**. In this step you will confirm that CLIENT1 is able to automatically re-enable the Windows Firewall after you manually disable it.
* **STEP 11: Demonstrate NAP Functionality for CLIENT1 When Connected to the HomeNet Network**. In this step you will confirm that you received a new health certificate after connecting to the Internet.
* **STEP 12: Verify CLIENT1 Cannot Connect to Intranet Resources when it is Non-Compliant**. In this step you will confirm that when CLIENT1 does meet health requirements it will not be able to connect to resources through the DirectAccess intranet tunnel.
* **Step 13:** After completing the Test Lab, take a snapshot of the working UAG DirectAccess with NAP Test Lab so that you can return to it later to test additional scenarios.

Note

You will notice that there are several steps that begin with an asterisk (\*). The \* indicates that the step requires that you move to a computer or virtual machine that is different from the computer or virtual machine you were at when you completed the previous step.

## STEP 1: Complete the Demonstrate UAG DirectAccess Test Lab Guide

The first step is to complete all the steps in the [Test Lab Guide: Demonstrate UAG DirectAccess](http://go.microsoft.com/fwlink/?LinkID=198436). After completing the steps in that Test Lab Guide you will have the core infrastructure required to complete this Test Lab Guide on how to configure UAG DirectAccess NLB enabled arrays. If you have already completed the steps in that Test Lab Guide and saved a snapshot or disk image of the Test Lab, you can restore the snapshot or image and begin with the next step.

## STEP 2: Install Update 1 on UAG1

You will install UAG Update 1 to bring UAG up to date for full NAP enforcement functionality.

1. Download UAG Update 1 and copy it the UAG1 computer or virtual machine. Follow the instructions on the UAG Update 1 to install the update.
2. Restart UAG1 after installation is complete and log on **CORP\User1**.

## STEP 3: Install the CA Server Role on APP1

In this step you will install a subordinate Certification Authority on APP1 so that it will be able to create health certificates requested by HRA on DC1 for DirectAccess NAP clients.

1. \*At the APP1 computer or virtual machine, in Server Manager, under **Roles Summary**, click **Add Roles**, and then click **Next**.
2. On the **Select Server Roles** page, select the **Active Directory Certificate Services** check box, and click **Next**.
3. On the **Introduction to Active Directory Certificate Services** page, click **Next**.
4. On the **Select Role Services** page, verify that the **Certification Authority** check box is selected, and then click **Next**.
5. On the **Specify Setup Type** page, click **Standalone**, and then click **Next**.
6. On the **Specify CA Type** page, click **Subordinate CA**, and then click **Next**.
7. On the **Set Up Private Key** page, click **Create a new private key**, and then click **Next**.
8. On the **Configure Cryptography for CA** page, click **Next**.
9. On the **Configure CA Name** page, under **Common name for this CA**, type **corp-APP1-SubCA**, and then click **Next**.
10. On the **Request Certificate from a Parent CA** page, choose **Send a certificate request to a parent CA**, and then click **Browse**.
11. In the **Select Certification Authority** dialog box, click **corp-DC1-CA**, and then click **OK**.
12. Verify that **DC1.corp.contoso.com\corp-DC1-CA** is displayed next to **Parent CA**, and then click **Next**.
13. Click **Next** to accept the default database settings, and then click **Install**.
14. Verify that all installations were successful, and then click **Close**

## STEP 4: Configure the Subordinate CA and CA Permissions on APP1

In this step you will configure the subordinate CA on APP1 so that it will automatically grant certificates when requested by DC1. You will also configure permissions on the CA to enable DC1 to issue and manage certificates, manage the CA and request certificates.

1. On the APP1 computer or virtual machine, click **Start**, type **certsrv.msc**, and then press ENTER.
2. In the Certification Authority console tree, right-click **corp-APP1-SubCA**, and then click **Properties**.
3. Click the **Policy Module** tab, and then click **Properties**.
4. Choose **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate**, and then click **OK**.
5. When you are prompted that AD CS must be restarted, click **OK** twice.
6. In the console tree, right-click **corp-APP1-SubCA**, point to **All Tasks**, and then click **Stop Service**.
7. Right-click **corp-APP1-SubCA**, point to **All Tasks**, and then click **Start Service**
8. In the console tree of the Certification Authority snap-in, right-click corp-APP1-SubCA, and then click Properties.
9. Click the Security tab, and then click Add.
10. Click **Object Types**, select **Computers**, and then click **OK**.
11. Type **DC1**, and then click **OK.**
12. Click **DC1**, select the Issue and Manage Certificates, Manage CA, and Request Certificates check boxes under **Allow**, and then click OK.
13. Close the Certification Authority console

## STEP 5: Install the NPS and HRA Server Roles on DC1

In this step you will install the Network Policy Server and Health Registration Authority Server roles on DC1.

1. \*At the DC1 computer or virtual machine, in Server Manager, under **Roles Summary**, click **Add Roles**, and then click **Next**.
2. On the **Select Server Roles** page, select the **Network Policy and Access Services** check box, and then click **Next** twice.
3. On the **Select Role Services** page, select the **Network Policy Server** and **Health Registration Authority** check boxes, click **Add Required Role Services** in the **Add Roles Wizard** window, and then click **Next**.
4. On the **Choose the Certification Authority to use with the Health Registration Authority** page, choose **Use an existing remote CA**, and then click **Select**.
5. In **Select Certification Authority**, click **corp-APP1-SubCA**, and then click **OK**. Click **Next**.
6. On the **Choose Authentication Requirements for the Health Registration Authority** page, choose **No, allow anonymous requests for health certificates**, and then click **Next**. This choice allows computers to be enrolled with health certificates in a workgroup environment.
7. On the **Choose a Server Authentication Certificate for SSL Encryption** page, click **Choose an existing certificate for SSL encryption (recommended)**, click the certificate named **DC1.corp.contoso.com**, and then click **Next**.
8. On the **Web Server (IIS)** page, click **Next**.
9. On the **Select Role Services** page, click **Next**.
10. On the **Confirm Installation Selections** page, click **Install**.
11. Verify that all installations were successful, and then click **Close**.

## STEP 6: Configure the NAP Health Policy Server on DC1

In this step you will configure NAP IPsec with HRA enforcement and enable Autoremediation for DirectAccess NAP clients. You will also configure the Windows Security Health Validator to require a firewall to be enabled for all network connections.

1. On the DC1 computer or virtual machine, click **Start**, type **nps.msc**, and then press ENTER.
2. In the details pane, under **Standard Configuration**, click **Configure NAP**.
3. On the **Select Network Connection Method for Use with NAP** page, under **Network connection method**, select **IPsec with Health Registration Authority (HRA)**, and then click **Next**.
4. On the **Specify NAP Enforcement Servers Running HRA** page, click **Next**. Because this NAP health policy server has an HRA installed locally, we do not need to add NAP enforcement servers.
5. On the **Configure User Groups and Machine Groups** page, click **Next**. You do not need to configure groups for this test lab.
6. 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**.
7. On the **Completing NAP Enforcement Policy and RADIUS Client Configuration** page, click **Finish**.
8. In the Network Policy Server console tree, open **Network Access Protection\System Health Validators\Windows Security Health Validator,** and then click **Settings**.
9. In the details pane, double click **Default Configuration**.
10. In the **Windows Security Health Validator** window, for the **Windows 7/Windows Vista**, clear all check boxes except **A firewall is enabled for all network connections**, and then click **OK.** Leave the Network Policy Server console open for a subsequent procedure.

## STEP 7: Reconfigure the DirectAccess Settings on UAG1

In this step you will reconfigure the DirectAccess settings on UAG1 to support NAP policy enforcement for DirectAccess clients. After you complete this step, the Connection Security Rule on the UAG DirectAccess server that controls access to the intranet tunnel will require DirectAccess clients to present a health certificate to successfully authenticate.

1. \*At the UAG1 computer or virtual machine, click **Start** and then click **All Programs**. Click **Microsoft Forefront UAG** and then click **Forefront UAG Management**.
2. In the **User Account Control** dialog box, click **Yes**.
3. In the **Microsoft forefront Unified Access Gateway Management** console, click the **DirectAccess** node in the left pane.
4. In the right pane of the console, in the **DirectAccess Server** section, click the **Edit** button.
5. On the **Connectivity** page, click **Next**.
6. On the **Managing DirectAccess Services** page, click **Next**.
7. On the **Authentication Options** page, put a checkmark in the **Computers that comply with your organizations NAP policy** checkbox. Click **Finish**.
8. Click the **Generate Policies** button.
9. On the **Forefront UAG DirectAccess Configuration Review** page, click **Apply Now**.
10. In the **DirectAccess Policy Configuration** window, click **OK**.
11. Click **Close** in the **Forefront UAG DirectAccess Configuration Review** page.
12. Open an elevated command prompt window and enter **gpupdate /force**. Close the command prompt windows after group policy is updated.
13. In the **Microsoft Forefront Unified Access Gateway Management** console, click the **File** menu and click **Activate**.
14. On the **Activate Configuration** page, click **Activate**.
15. On the **Activate Configuration** page, click **Finish**.
16. Close the **Microsoft Forefront Unified Access Gateway Management** console.
17. Click **Yes** in the dialog box that asks if you want to close the console.
18. Click **Start** and enter **wf.msc** in the Search box and press ENTER.
19. In the **Windows Firewall with Advanced Security** console, navigate to the **Windows Firewall with Advanced Security\Monitoring\Connection Security Rules** node in the left pane. Double click on the **UAG DirectAccess Gateway – Clients Access Enabling Tunnel All**. In the dialog box, click on the **Authentication** tab. In the **First authentication** section expand the **Details** column. Notice the details include **Root CA, RSA Certificate Signing**. Click **Cancel**. This is the Connection Security Rule used to access the infrastructure tunnel.
20. Double click the **UAG DirectAccess Gateway – Clients Corp Tunnel** Connection Security Rule. In the dialog box, click the **Authentication** tab. In the **First authentication** section, expand the **Details** section. Scroll the section to the right and notice the entry **Accept only health certificates**. This indicates that the DirectAccess client will need to present a valid health certificate to establish the intranet tunnel. Click **Cancel**.
21. Close the **Windows Firewall with Advanced Security** console.

## STEP 8: Configure NAP Client Settings in Group Policy

In this step you will configure a number of Group Policy settings in the UAG DirectAccess clients GPO that are required by Network Access Protection clients. Note that in a production environment, you should create a separate GPO and OU for the DirectAccess clients and apply these settings to the separate GPO. The reason for this is that each time you run the UAG DirectAccess wizard, the DirectAccess clients GPO created by the wizard is overwritten and you will lose your custom settings.

1. \*On the DC1 computer or virtual machine, click **Start**, type **gpme.msc**, and then press ENTER.
2. In the **Browse for a Group Policy Object** dialog box, double-click the policy named **UAG DirectAccess: Client{3491980e-ef3c-4ed3-b176-a4420a810f12}**.
3. In the console tree of Group Policy Management Editor, open **Computer Configuration\Policies\Windows Settings\Security Settings**, and then click **System Services**.
4. In the details pane, double-click **Network Access Protection Agent**.
5. In the **Network Access Protection Agent Properties** dialog box, select **Define this policy setting**, click **Automatic**, and then click **OK**.
6. In the console tree, open **Computer Configuration\Policies\Windows Settings\Security Settings\Network Access Protection\NAP Client Configuration**, and then click **Enforcement Clients**.
7. In the details pane, right-click **IPsec Relying Party**, and then click **Enable**.
8. In the console tree under **NAP Client Configuration**, open **Health Registration Settings**.
9. Right-click **Trusted Server Groups** and then click **New**.
10. In the **Group Name** window, type **Trusted HRA Servers**, and then click **Next**.
11. In the **Add Servers** window, under **Add URLs of the health registration authority that you want the client to trust**, type **https://dc1.corp.contoso.com/domainhra/hcsrvext.dll**,and then click **Add**. This is the Web site that will process domain-authenticated requests for health certificates.
12. Verify the URL you typed. The URL must be correct or the client computer will be unable to request a system health validation and health certificate.
13. Click **Finish** to complete the process of adding HRA trusted server groups.
14. In the console tree, open **Computer Configuration\Policies\Administrative Templates\Windows Components**, and then click **Security Center**.
15. In the details pane, double-click **Turn on Security Center (Domain PCs only)**, click **Enabled**, and then click **OK**. This enables the Windows Action Center on DirectAccess clients.
16. Close the **Group Policy Management Editor** window.

## STEP 9: Verify NAP Health Evaluation for CLIENT1

In this step you will confirm that CLIENT1 received the Group Policy settings required for NAP clients and confirm that CLIENT1 received a health certificate from DC1.

1. \*Connect CLIENT1 to the Corpnet subnet. Wait until the network icon in the notification area of the desktop displays a yellow caution sign.
2. Click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**. Click **Yes** at the **User Account Control** prompt.
3. In the command prompt window, run the **gpupdate /target:computer** command.
4. In the command prompt window, run the **netsh nap client show grouppolicy** command.
5. In **Enforcement clients**, **IPsec Relying Party** should be set to **Enabled**.
6. In **Trusted server group configuration**, **URL** should be set to **https://dc1.corp.contoso.com/domainhra/hcsrvext.dll**.
7. Click **Start**, type **mmc,** and then press ENTER. Click **Yes** at the **User Account Control** prompt.
8. Click **File**, and then click **Add/Remove Snap-ins**.
9. Click **Certificates**, click **Add**, click **Computer account**, click **Next**, select **Local computer**, click **Finish**, and then click **OK**.
10. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**.
11. In the contents pane, double-click the certificate issued by **corp-APP1-SubCA**.
12. Click the **Details** tab, and then click the **Enhanced Key Usage** field. You should see **System Health Authentication** in the list. Click **OK**. Leave the Certificates snap-in window open for a later procedure.

## STEP 10: Verify NAP Autoremediation Functionality for CLIENT1

In this step you will confirm that CLIENT1 is able to automatically re-enable the Windows Firewall after you manually disable it.

1. On CLIENT1, click **Start**, enter **wf.msc** in the Searchbox and press ENTER.
2. In the right pane of the console, click **Properties**.
3. In the **Windows Firewall with Advanced Security** dialog box, click the **Domain Profile** tab.
4. On the **Domain Profile** tab, click the down-arrow for the **Firewall state** drop down box and click **Off**. Click **OK**.
5. Click **Refresh** in the right pane. Notice that the NAP client automatically turns on Windows Firewall for domain networks.
6. \*On DC1, in the console tree of the Network Policy Server snap-in, open **Network Access Protection\System Health Validators\Windows Security Health Validator\Settings**.
7. In the details pane, double-click **Default configuration**.
8. Select **An antivirus application is on**, and then click **OK**.
9. \*On CLIENT1, in the **Windows Firewall with Advanced Security** console, click **Properties** in the right pane.
10. In the **Windows Firewall with Advanced Security** dialog box, on the **Domain Profile** tab, click the down-arrow in the **Firewall state** drop down box and click **Off**. Click **OK**.
11. Notice that the NAP client automatically turns on Windows Firewall for domain networks. However, this time you should see a persistent **Network Access Protection: Network access might be limited** message in the notification area of the desktop.
12. This indicates that CLIENT1 is not compliant with system health requirements. There is no antivirus program installed on CLIENT1.
13. Click the notification message or if the notification message disappears, click the Action Center icon (the flag icon) in the system notification area and click **Network Access Protection (Important)**. In the **Network Access Protection** window, you should see the message **This computer doesn’t meet security standards defined by your network administrator**.
14. In the Certificates snap-in window, press F5 to refresh the list of installed certificates. Notice that there is no longer a certificate issued by corp-APP1-SubCA.
15. \*On DC1, in the details pane of the Network Policy Server snap-in, double-click **Default configuration**.
16. Clear **An antivirus application is on**, and then click **OK**.
17. \*On CLIENT1, in the **Network Access Protection** window, click **Try Again**. You should see the message **This computer meets security standards defined by your network administrator**. Click **Close**.
18. In the Certificates snap-in window, press F5 to refresh the list of installed certificates. Notice that there is a new certificate issued by corp-APP1-SubCA.
19. Double-click the certificate issued by corp-APP1-SubCA, click the **Details** tab, and then click the **Valid from** field. Note the date and time that the certificate was issued.

## STEP 11: Demonstrate NAP Functionality for CLIENT1 When Connected to HomeNet

In this step you will confirm that you received a new health certificate after connecting to the Homenet network.

1. On CLIENT1, open an elevated command prompt and enter **netsh interface teredo set state default** and press ENTER. This is to insure that CLIENT1 is able to establish a Teredo connection when behind NAT1.
2. Connect CLIENT1 to the Homenet subnet. Wait until the network icon in the notification area of the desktop displays a yellow caution sign.
3. In the contents pane of the Certificates snap-in, press F5. You should see a health certificate issued by corp-APP1-SubCA. Double-click the certificate issued by corp-APP1-SubCA, click the **Details** tab, and then click the **Valid from** field. Notice that the date and time that the certificate issue date and time is newer than in the previous procedure. This indicates that a new health certificate was issued by APP1 over the DirectAccess connection. Click **OK**.
4. In the **Windows Firewall with Advanced Security** console, click **Properties** in the right pane.
5. In the **Windows Firewall with Advanced Security** dialog box, on the **Domain Profile** tab, click the down-arrow in the **Firewall state** drop down box and click **Off**. Click **OK**.
6. Click **Refresh** in the right pane of the console. Notice that the Windows Firewall is automatically turned on.
7. Watch as the NAP client automatically turns on Windows Firewall for domain networks.

## STEP 12: Verify CLIENT1 Cannot Connect to Intranet Resources when it is Non-Compliant

In this step you will confirm that when CLIENT1 does meet health requirements it will not be able to connect to resources through the DirectAccess intranet tunnel. In the test lab, DC1 is accessible through the infrastructure tunnel and APP1 is accessible through the intranet tunnel. When the UAG DirectAccess NAP client fails validation, it can only access resources available through the infrastructure tunnel.

1. In the **Windows Firewall with Advanced Security** console, click **Properties** in the right pane.
2. In the **Windows Firewall with Advanced Security** dialog box, on the **Domain Profile** tab, click the down-arrow in the **Firewall state** drop down box and click **Off**. Click **OK**.
3. Watch as the NAP client automatically turns on Windows Firewall for domain networks.
4. \*On DC1, in the console tree of the Network Policy Server snap-in, open **Network Access Protection\System Health Validators\Windows Security Health Validator\Settings**.
5. In the details pane, double-click **Default configuration**.
6. Select **An antivirus application is on**, and then click **OK**.
7. \*On CLIENT1, In the **Windows Firewall with Advanced Security** console, click **Properties** in the right pane.
8. In the **Windows Firewall with Advanced Security** dialog box, on the **Domain Profile** tab, click the down-arrow in the **Firewall state** drop down box and click **Off**. Click **OK**.
9. Click **Refresh** in the right pane of the console. The NAP client automatically turns on Windows Firewall for domain networks. However, this time you should see a persistent **Network Access Protection: Network access might be limited** message in the notification area of the desktop. This indicates that CLIENT1 is not compliant with system health requirements. There is no antivirus program installed on CLIENT1. If you do not see a persistent message, click the Action Center icon in the system notification area (the flag icon) and click the **Network Access Protection (Important)** link.
10. Click the notification message or Action Center link. In the **Network Access Protection** window, you should see the message **This computer doesn’t meet security standards defined by your network administrator**.
11. In the Command Prompt window, run the **net view \\app1** command. You should see the error message **The network path was not found.** Because CLIENT1 no longer has a health certificate, it cannot perform authentication for the intranet tunnel and access intranet resources.
12. \*On DC1, in the details pane of the Network Policy Server snap-in, double-click **Default configuration**.
13. Clear **An antivirus application is on**, and then click **OK**.
14. \*On CLIENT1, in the **Network Access Protection** window, click **Try Again**. You should see the message **This computer meets security standards defined by your network administrator**. Click **Close**.
15. In the Command Prompt window, run the **net view \\app1** command. You should see the list of shares on APP1. CLIENT1 is once again compliant with system health requirements and is able to access computers, such as APP1, which are reachable only through the intranet tunnel.

## STEP 13: Snapshot the Configuration

This completes the DirectAccess test lab. To save this configuration so that you can quickly return to a working DirectAccess configuration from which you can test other DirectAccess modular TLGs, TLG extensions, or for your own experimentation and learning, do the following:

1. On all physical computers or virtual machines in the test lab, close all windows and then perform a graceful shutdown.
2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots **UAG DirectAccess with NAP**. If your lab uses physical computers, create disk images to save the DirectAccess test lab configuration.

# Additional Resources

For procedures to configure the Base Configuration test lab on which this document is based, see the [Test Lab Guide: Base Configuration](http://go.microsoft.com/fwlink/?LinkId=198140).

For procedures to demonstrate additional DirectAccess functionality using the DirectAccess test lab described in this document, see the “DirectAccess Test Lab Extensions” section of [DirectAccess Test Lab for Windows Server 2008 R2](http://social.technet.microsoft.com/wiki/contents/articles/directaccess-test-lab-for-windows-server-2008-r2.aspx).

For the design and configuration of your pilot or production deployment of DirectAccess, see the [Forefront UAG DirectAccess design guide](http://technet.microsoft.com/en-us/library/ee406191.aspx) and the [Forefront UAG DirectAccess deployment guide](http://technet.microsoft.com/en-us/library/dd857320.aspx).

For information about troubleshooting DirectAccess, see the [DirectAccess Troubleshooting Guide](http://go.microsoft.com/fwlink/?LinkId=165904).

For more information about DirectAccess, see the [DirectAccess Getting Started Web page](http://www.microsoft.com/servers/directaccess.mspx) and the [DirectAccess TechNet Web page](http://technet.microsoft.com/en-us/network/dd420463.aspx).