





Test Lab Guide: Demonstrate Forefront UAG SP1 RC DirectAccess with Network Access Protection (NAP)

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 SP1 RC extends the 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 SP1 RC DirectAccess](http://go.microsoft.com/fwlink/?LinkId=204993) 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.

Author: Thomas W Shinder (tomsh@microsoft.com)

Last Updated October 30, 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](#_Toc276363317)

[In this guide 2](#_Toc276363318)

[Overview of the test lab scenario 2](#_Toc276363319)

[Configuration component requirements 3](#_Toc276363320)

[Steps for configuring the test lab 5](#_Toc276363321)

[STEP 1: Complete the Demonstrate UAG SP1 RC DirectAccess Test Lab Guide 6](#_Toc276363322)

[STEP 2: Install the CA Server Role on APP1 6](#_Toc276363323)

[STEP 3: Configure the Subordinate CA and CA Permissions on APP1 7](#_Toc276363324)

[STEP 4: Configure UAG1 as a NPS Server and NAP Health Registration Authority (HRA) 8](#_Toc276363325)

[STEP 5: Verify NAP Configuration on CLIENT1 9](#_Toc276363326)

[STEP 6: Install Microsoft Security Essentials on CLIENT1 9](#_Toc276363327)

[STEP 7: Confirm that CLIENT1 Passes NAP Evaluation 10](#_Toc276363328)

[STEP 8: Confirm that CLIENT1 cannot access the Intranet Tunnel when NAP Non-Compliant 11](#_Toc276363329)

[STEP 9: Snapshot the Configuration 12](#_Toc276363330)

[Additional Resources 13](#_Toc276363331)

# 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) SP1 RC 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 SP1 RC 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.

Combining 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).

UAG DirectAccess SP1 RC enables you to deploy DirectAccess and NAP in two different ways. You can deploy a NAP infrastructure on your intranet that can be used by all systems on your network where the NAP infrastructure components are installed on one or more servers on your intranet. This option was available prior to UAG DirectAccess SP1 RC. A new option available with UAG DirectAccess SP1 RC is the ability to host the NAP server (Network Policy Server) and the Health Registration Authority on the UAG servers themselves. This option is useful if you don’t already have an established NAP deployment and want to focus your NAP design on DirectAccess clients only. We will enable the new NAP option in this Test Lab Guide.

## In this guide

This guide provides step-by-step instructions for configuring UAG DirectAccess SP1 RC with NAP in a test lab so that you can see how it works. You will set up and deploy UAG DirectAccess SP1 RC 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 with NAP. The starting point for this paper is the [Test Lab Guide: Demonstrate UAG SP1 RC DirectAccess](http://go.microsoft.com/fwlink/?LinkId=204993) .

|  |
| --- |
| **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 SP1 RC 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 a Forefront UAG DirectAccess SP1 RC server.
* One intranet member server running Windows Server 2008 R2 Enterprise Edition (APP1) that is configured as a general application server and network location server.
* 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 UAG’s 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 domain 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 subnet by NAT1.
* The Internet subnet (131.107.0.0/24).
* The Corpnet subnet (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 (NAT1).
* The product disc or a downloaded version of Microsoft Forefront Unified Access Gateway (UAG) SP1 RC.
* Access to a live network where CLIENT1 can be temporarily attached to download Microsoft Security Essentials and update the antimalware signatures.

This Test Lab Guide demonstrates UAG DirectAccess SP1 RC with NAP in full enforcement mode where the UAG DirectAccess SP1 RC server requires health certificates for authentication to access resources through the intranet tunnel. Noncompliant UAG DirectAccess SP1 RC clients cannot access the intranet and cannot use their computer certificate for authentication of the intranet tunnel.

For more information about the different modes of NAP, see [Stages of a NAP Deployment](http://technet.microsoft.com/en-us/library/dd125311%28WS.10%29.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 CLIENT1 for UAG DirectAccess SP1 RC with NAP. After UAG1, APP1 and CLIENT1 are configured, this guide provides steps for demonstrating NAP functionality for CLIENT1 when it is connected to the Homenet subnet.

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 SP1 RC DirectAccess](http://go.microsoft.com/fwlink/?LinkId=204993).

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

* **Step 1: Complete the Demonstrate UAG SP1 RC DirectAccess Test Lab Guide –** The first step is to complete all the steps in the [Test Lab Guide: Demonstrate UAG SP1 RC DirectAccess](http://go.microsoft.com/fwlink/?LinkId=204993).
* **STEP 2: 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 3: 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 UAG1, which is configured as a Health Registration Authority. You will also configure permissions on the CA to enable UAG1 to issue and manage certificates, manage the CA and request certificates.
* **STEP 4: Configure UAG1 as an NPS Server and NAP health Registration Authority (HRA)**. In this step you will reconfigure the DirectAccess settings on UAG1 to support NAP policy enforcement for DirectAccess clients. After you complete this step, UAG1 will be configured as a Network Policy Server that provides NAP server functionality, as well as a Health Registration Server (HRA).
* **STEP 5: Verify NAP Configuration on 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 UAG1.
* **STEP 6: Install Microsoft Security Essentials on CLIENT1**. In this step you will connect CLIENT1 to a live portion or your network so that it can download and install Microsoft Security Essentials.
* **STEP 7: Confirm that CLIENT1 Passes NAP Evaluation**. In this step you will move CLIENT1 to the Homenet subnet and confirm that CLIENT1 can pass NAP evaluation and access resources on the intranet through the intranet tunnel.
* **STEP 8: Confirm that CLIENT1 cannot access the Intranet Tunnel when NAP Non-Compliant**. In this step you will confirm that when CLIENT1 does not meet health requirements it will not be able to connect to resources through the DirectAccess intranet tunnel.
* **Step 9:** **Snapshot the configuration**. 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 SP1 RC DirectAccess Test Lab Guide

The first step is to complete all the steps in the [Test Lab Guide: Demonstrate UAG SP1 RC DirectAccess](http://go.microsoft.com/fwlink/?LinkId=204993). 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 with NAP. 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 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 the Health Registration Authority (HRA) on UAG1 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**, enter **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 3: 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 UAG1. You will also configure permissions on the CA to enable UAG1 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 4: Configure UAG1 as a NPS Server and NAP Health Registration Authority (HRA)

In this step you will reconfigure the DirectAccess settings on UAG1 to support NAP policy enforcement for DirectAccess clients. After you complete this step, UAG1 will be configured as a Network Policy Server that provides NAP server functionality, as well as a Health Registration Server (HRA). In addition 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 **Step 2 DirectAccess Server** section, click the **Network Access Protection** link.
5. This starts the **Network Access Protection Configuration** wizard. On the **NAP Enforcement** page, put a checkmark in the **Use NAP to verify DirectAccess client computers are compliant with network health policies** checkbox, and then select the **Enforcement mode. Only compliant DirectAccess client can connect** option. Click **Next**.
6. On the **HRA and NPS** page, select the **The NPS and HRA roles are installed on this UAG server (UAG configures settings automatically)** option. Put a checkmark in the **Use Autoremediation to automatically update non-compliant computers** checkbox. In the **Clients can link to this URL for troubleshooting compliance issues (optional)** text box, enter [**http://www.contoso.com/troubleshooting.txt**](http://www.contoso.com/troubleshooting.txt)**.** Click **Next**.
7. On the **NAP Certification Authority** page, click the **Add** button. In the **Add a CA Server** dialog box, click the **Browse** button. In the **Select a CA server** dialog box, click **APP1.corp.contoso.com\corp-APP1-SubCA**, and then click **OK**. In the **Add a CA Server** dialog box, click **OK**. Click **Finish**.
8. In the right pane of the console, click **Apply Policy**.
9. On the **Forefront UAG DirectAccess Configuration Review** page, click **Apply Now**.
10. In the **DirectAccess Policy Configuration** dialog box, click **OK** after you see it say **Script run completed with no errors or warnings**.
11. On the **Forefront UAG DirectAccess Configuration Review** page, click **Close**.
12. Open an elevated command prompt. In the **Command Prompt** window, enter **gpupdate /force** and press ENTER. Close the **Command Prompt** window after the command completes.
13. In the right pane of the console, click **Activate**.
14. In the **Activate Configuration** dialog box, click **Activate**. Click **Finish** when **Activation completed successfully**.

## STEP 5: Verify NAP Configuration on 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://uag1.contoso.com/domainhra/hcsrvext.dll**.

## STEP 6: Install Microsoft Security Essentials on CLIENT1

The UAG SP1 RC DirectAccess wizard has configured the SHV on the NAP server to use the default settings. One of these settings is to require that that a healthy client have an anti-virus application installed and that it is up to date. In this step you will connect CLIENT1 to a live portion or your network so that it can download and install Microsoft Security Essentials.

1. Move CLIENT1 to a live portion of your network and assign CLIENT1 a valid IP address that enables it to access the Internet to download Microsoft Security Essentials.
2. Open **Internet Explorer** and browse to [**https://www.microsoft.com/security\_essentials**](https://www.microsoft.com/security_essentials). On the **Security Essentials** web site, click **Download Now**.
3. Close **Internet Explorer** after the download is complete.
4. Double click on the **mssefullinstall-amd64fre-en-us-vista-win7** file that you downloaded.
5. In the **User Account Control** dialog box, click **Yes**.
6. On the **Welcome to the Microsoft Security Essentials 1.0 Installation Wizard** page, click **Next**.
7. On the **Microsoft Security Essentials License Agreement** page, click **I accept**.
8. On the **ready to install Microsoft Security Essentials** page, click **Install**.
9. On the **Completing the Microsoft Security Essentials Installation Wizard** page, click **Finish**.
10. In the **Microsoft Security Essentials** window, click the **Update** button.
11. After the update is complete, close the **Microsoft Security Essentials** window.

## STEP 7: Confirm that CLIENT1 Passes NAP Evaluation

In this step you will move CLIENT1 to a Homenet subnet and confirm that CLIENT1 can pass NAP evaluation and access resources on the intranet through the intranet tunnel.

1. Move CLIENT1 to the Homenet subnet.
2. Open an elevated command prompt. In the **Command Prompt** window, enter **napstat** and press ENTER. You will see a balloon that says **Network Access Protection You have full network access**. Close the **Command Prompt** window.
3. Click **Start,** enter **mmc** in the Search box and press ENTER. In the **User Account Control** dialog box, click **Yes**.
4. In the **Console** window, click **File** and click **Add/Remove Snap-in**.
5. In the **Add or Remove Snap-ins** dialog box, click **Certificates** and click **Add**.
6. In the **Certificates** dialog box, select **Computer account** and click **Next**.
7. In the **Select Computer** dialog box, select **Local computer** and click **Finish**.
8. In the **Add or Remove Snap-ins** dialog box, click **OK**.
9. In the left pane of the console window, navigate to **Certificates (Local Computer)\Personal\Certificates**. In the middle pane of the console, notice that there is a certificate issued by **corp-APP1-SubCA**. Double click on that certificate.
10. In the **Certificate** dialog box, on the **General** tab, note that in the **This certificate is intended for the following purposes(s):** section that one of the intended purposes is **System Health Authentication**. This indicates that CLIENT1 has passed NAP inspection and should now have access to the intranet tunnel.
11. In the **Certificate** dialog box, click **OK**. Minimize the **Console1** window.
12. Click **Start** and in the Search box, enter [**\\app3\files**](file:///%5C%5Capp3%5Cfiles) and press ENTER.
13. Double click on the **Example** file. You can now read the contents of that file. This confirms that you have access to the Corpnet subnet over the intranet tunnel, since APP1 is not a member of the infrastructure servers group. Close the Windows Explorer window that shows the contents of the **Files** share. Close the **Notepad** window.
14. Click **Start** and then enter **wf.msc** in the Search box and press ENTER.
15. In the middle pane of the console, note that the **Private Profile is Active**. DirectAccess clients will only establish their DirectAccess tunnels to the DirectAccess server when either the Public or Private Profiles are active.
16. In the right pane of the console, click **Properties**. In the **Windows Firewall with Advanced Security** dialog box, click the down arrow next to **Firewall state** and click **Off**. Click **OK**. You will see two balloons appear in the system notification area. One will ask that you turn on the Windows Firewall and the second will inform you that network access may be limited. Note in the middle pane that it says **Windows Firewall is off**. Click **Refresh** in the right pane. NAP auto-remediation automatically enabled the Windows Firewall after it was turned off.
17. In the left pane of the console, navigate to **Windows Firewall with Advanced Security\Monitoring\Security Associations\Main Mode**. Notice the Main Mode entry that has **User (Kerberos V5)** as the second authentication method. This indicates that the user was able to access the intranet tunnel since the intranet tunnel requires user authentication. In addition, when NAP is enabled for DirectAccess clients, the computer certificate used to authenticate the intranet tunnel is the Health Certificate, indicating that the computer was able to pass NAP inspection.
18. Minimize the **Windows Firewall with Advanced Security** window.

## STEP 8: Confirm that CLIENT1 cannot access the Intranet Tunnel when NAP Non-Compliant

In this step you will confirm that when CLIENT1 does not 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. On CLIENT1, click **Start** and then in the Search box, enter **services.msc** and press ENTER.
2. In the right pane of the **Services** console, double click on **Microsoft Antimalware Service**.
3. In the **Microsoft Antimalware Service Properties (Local Computer)** dialog box, click the **Stop** button. Click **OK** and then minimize the **Services** console.
4. Notice that a **Network Access Protection Network access might be limited** balloon appears. This indicates that CLIENT1 no longer passes NAP inspection. In the **Microsoft Security Essentials** dialog box, click the Close control button (the “x” in the upper right) to close the dialog box.
5. Restore the console window that has the **Certificates** snap in installed. Right click the middle pane and click **Refresh**. Notice that the health certificate no longer appears. When the client does not pass NAP inspection, the certificate is removed from the machine’s computer store.
6. Restore the **Windows Firewall with** **Advanced Security** console and click **Refresh** in the right pane of the console. Notice that the Main Mode security association using Kerberos V5 as the 2nd Authentication Method is no longer there. This indicates that the client is no longer able to establish the intranet tunnel because it cannot provide a health certificate for computer authentication.
7. Click **Start** and enter [**\\app1\files**](file:///%5C%5Capp1%5Cfiles) in the Search box and press ENTER. After a few moments you will see a **Network Error** dialog box indicating that Windows cannot access the share. This is consistent with the fact that CLIENT1 needs access to the intranet tunnel to access APP1 and the fact that the intranet tunnel is not available because CLIENT1 current does not pass NAP inspection. Click **Cancel** in the **Network Error** dialog box.
8. Click **Start** and enter [**\\dc1\files**](file:///%5C%5Cdc1%5Cfiles) in the Search box and press ENTER. In this case the **Files** share is available. The reason for this is that access to servers in the infrastructure servers list is accessible over the infrastructure tunnel.
9. Restore the **Services** console and right click **Microsoft Antimalware Service** and click **Start**.
10. Click **Start** and enter [**\\app1\files**](file:///%5C%5Capp1%5Cfiles) in the Search box and press ENTER. You can now access APP1 over the intranet tunnel because CLIENT1 is able to pass NAP inspection.
11. Close all open windows on CLIENT1 and do not save the changes to any of the mmc consoles.

## STEP 9: Snapshot the Configuration

This completes the UAG SP1 RC DirectAccess with NAP test lab. To save this configuration so that you can quickly return to a working UAG SP1 RC DirectAccess with NAP 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 **TLG UAG DirectAccess SP1RC 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 configure UAG SP1 RC DirectAccess on which this document is based, see the [Test Lab Guide: Demonstrate Forefront UAG SP1 RC DirectAccess](http://go.microsoft.com/fwlink/?LinkId=204993).

For a comprehensive list of UAG DirectAccess Test Lab Guides, please see [Test Lab Guides](http://social.technet.microsoft.com/wiki/contents/articles/test-lab-guides.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 information on troubleshooting UAG DirectAccess in a Test Lab, see [Test Lab Guide: Troubleshooting UAG DirectAccess](http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=d2e460c8-b4bf-4fda-9f86-ecc4b7add5d1).

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).