

**Test Lab Guide: Demonstrate DirectAccess Simplified Setup in an IPv4-only Test Environment in Windows Server "8" Beta**

Microsoft Corporation

Published: February 2012

**Abstract**

This paper contains an introduction to Windows Server "8" Beta Remote Access and step-by-step instructions for extending the Windows Server "8" Beta Base Configuration test lab to demonstrate Remote Access deployment using the Getting Started Wizard.

**Copyright information**

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious.  No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2012 Microsoft. All rights reserved.

Active Directory, Hyper-V, Microsoft, MS-DOS, Visual Basic, Visual Studio, Windows, Windows NT, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[Introduction 5](#_Toc317798807)

[In this guide 5](#_Toc317798808)

[Test lab overview 6](#_Toc317798809)

[Hardware and software requirements 7](#_Toc317798810)

[Steps for Configuring the Remote Access Test Lab 8](#_Toc317798811)

[Step 1: Set up the Base Configuration Test Lab 9](#_Toc317798812)

[Step 2: Configure DC1 9](#_Toc317798813)

[Create a security group for DirectAccess client computers 9](#_Toc317798814)

[Step 3: Configure EDGE1 10](#_Toc317798815)

[Install the Remote Access server role on EDGE1 10](#_Toc317798816)

[Deploy simplified DirectAccess using the Getting Started Wizard 11](#_Toc317798817)

[Step 4: Configure CLIENT1 12](#_Toc317798818)

[Connect CLIENT1 to the Corpnet subnet and update group policy 13](#_Toc317798819)

[Connect CLIENT1 to the Internet subnet and test remote access 13](#_Toc317798820)

[Connect CLIENT1 to the Homenet subnet and test remote access 15](#_Toc317798821)

[Monitor the client connection on the EDGE1 DirectAccess server 16](#_Toc317798822)

[Snapshot the Configuration 16](#_Toc317798823)

[Additional Resources 17](#_Toc317798824)

# Introduction

DirectAccess provides users with the experience of being seamlessly connected to their intranet any time they have Internet access. When DirectAccess is enabled, requests for intranet resources (such as email servers, shared folders, or intranet websites) are securely directed to the intranet, without the need for users to connect to a VPN. DirectAccess enables increased productivity for a mobile workforce by offering the same connectivity experience both inside and outside of the office.

The Windows Routing and Remote Access Server (RRAS) provides traditional VPN connectivity for legacy clients and non-domain members. RRAS also provides site-to-site connections between servers. RRAS in Windows Server 2008 Beta R2 cannot coexist on the same edge server with DirectAccess, and must be deployed and managed separately from DirectAccess.

Windows Server "8" Beta combines the DirectAccess feature and the RRAS role service into a new unified server role. This new Remote Access server role allows for centralized administration, configuration, and monitoring of both DirectAccess and VPN-based remote access services. Additionally, Windows Server "8" Beta DirectAccess provides multiple updates and improvements to address deployment blockers and provide simplified management.

Administrators can now deploy DirectAccess using a new Getting Started Wizard, which presents a greatly simplified configuration experience. The Getting Started Wizard masks the complexity of DirectAccess, and allows for an automated setup in a few simple steps. The administrator no longer requires an understanding of the technical details of things like IPv6 transition technologies and Network Location Server (NLS) deployment.

The new setup wizard provides a seamless experience for the administrator by configuring Kerberos proxy automatically to eliminate the need for an internal PKI deployment. In this simplified DirectAccess deployment, user level configuration options such as force tunneling, Network Access Protection (NAP) integration, and two-factor authentication are not available. However, it is possible to modify the simplified deployment later by running the Remote Access Setup Wizard, which provides support for all DirectAccess deployment options.

## In this guide

This guide provides step-by-step instructions for configuring DirectAccess using the Getting Started Wizard in a test lab to demonstrate functionality of the simplified deployment experience. You will set up and deploy DirectAccess based on the Windows Server "8" Beta Base Configuration using five server computers and two client computers. The resulting test lab simulates an intranet, the Internet, and a home network, and demonstrates DirectAccess in different Internet connection scenarios.

Important

The following instructions are for configuring a Remote Access 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.

Attempting to adapt this Remote Access test lab configuration to a pilot or production deployment can result in configuration or functionality issues.

## Test lab overview

In this test lab, Remote Access is deployed with:

* One computer running Windows Server "8" Beta named DC1 that is configured as an intranet domain controller, Domain Name System (DNS) server, and Dynamic Host Configuration Protocol (DHCP) server
* One intranet member server running Windows Server "8" Beta named EDGE1 that is configured as a DirectAccess server
* One intranet member server running Windows Server "8" Beta named APP1 that is configured as a general application server and web server
* One standalone server running Windows Server "8" Beta named INET1 that is configured as an Internet DHCP server, DNS server, and web server
* One roaming member client computer running Windows 8 Consumer Preview named CLIENT1 that is configured as a DirectAccess client
* One standalone client computer running Windows 8 Consumer Preview named NAT1 that is configured as a network address translation (NAT) device using Internet Connection Sharing

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

* The Internet (131.107.0.0/24).
* An intranet named Corpnet (10.0.0.0/24) separated from the Internet by EDGE1.
* A home network named Homenet (192.168.137.0/24) connected to the Internet subnet by a NAT

Computers on each subnet connect using a hub or switch. See the following figure.

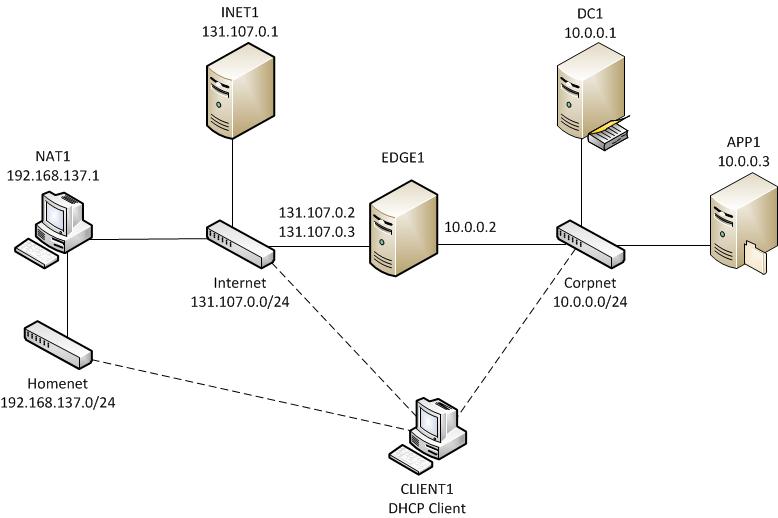


Figure 1 DirectAccess Getting Started wizard IPv4-only lab configuration

Windows Server "8" Beta DirectAccess does not require IPv6 deployment or a PKI infrastructure to deploy a simplified remote access solution. This modular test lab demonstrates DirectAccess in an IPv4-only environment with no existing certificates. A test client computer is used to show connectivity to corporate resources via a simulated corporate network (the Corpnet subnet), simulated Internet (the Internet subnet), and a simulated home network behind a NAT (the Homenet subnet).

## Hardware and software requirements

The following are required components of the test lab:

* The product disc or files for Windows Server "8" Beta
* The product disc or files for Windows 8 Consumer Preview
* Five computers or virtual machines that meet the minimum hardware requirements for Windows Server "8" Beta

# Steps for Configuring the Remote Access Test Lab

There are four steps to follow when setting up a Remote Access express setup test lab based on the Test Lab Guide Base Configuration.

1. Set up the Base Configuration test lab.

The Remote Access simplified setup test lab requires the [Test Lab Guide: Windows Server "8" Beta Base Configuration](http://go.microsoft.com/fwlink/p/?LinkId=236358) with [Optional mini-module: Homenet subnet](http://go.microsoft.com/fwlink/p/?LinkId=244230), as its starting point.

1. Configure DC1.

DC1 is already configured as a domain controller with Active Directory, and as the DNS and DHCP server for the intranet subnet. For the DirectAccess simplified setup test lab, a security group will be added to Active Directory for DirectAccess client computers.

1. Configure EDGE1.

EDGE1 is already a member server computer. For the Remote Access express setup test lab, EDGE1 must be configured as a Remote Access server with simplified DirectAccess deployed.

1. Configure CLIENT1.

CLIENT1 is already a domain member client computer running Windows 8 Consumer Preview. For the Remote Access express setup test lab, CLIENT1 will be used to test and demonstrate remote access operation.

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.

This guide provides steps for configuring the computers of the Windows Server "8" Beta Base Configuration test lab, configuring Remote Access in Windows Server "8" Beta, and demonstrating remote client connectivity. The following sections provide details about how to perform these tasks.

## Step 1: Set up the Base Configuration Test Lab

Set up the Base Configuration test lab for both the Corpnet and Internet subnets using the procedures in the “Steps for Configuring the Corpnet Subnet” and “Steps for Configuring the Internet Subnet” sections of the [Test Lab Guide: Windows Server "8" Beta Base Configuration](http://go.microsoft.com/fwlink/p/?LinkId=236358).

Set up the Homenet subnet using the procedures in the [Optional mini-module: Homenet subnet](http://go.microsoft.com/fwlink/p/?LinkId=244230).

Do *NOT* complete the procedures in the [Optional mini-module: Basic PKI](http://go.microsoft.com/fwlink/p/?LinkId=244229). This Remote Access test lab demonstrates the ability to deploy DirectAccess in an environment without a PKI deployment.

## Step 2: Configure DC1

DC1 configuration for the Remote Access express setup test lab consists of the following procedure:

* Create a security group for DirectAccess client computers

The following section explains this procedure in detail.

### Create a security group for DirectAccess client computers

When DirectAccess is configured, it automatically creates group policy objects containing DirectAccess settings, and these are applied to DirectAccess clients and servers. By default, the Getting Started Wizard applies the client GPO to mobile computers only, in the Domain Computers security group. The procedures in this lab do not use the default setting, but instead create an alternate security group for DirectAccess clients.

To create a DirectAccess client security group

|  |
| --- |
| 1. On **DC1**, from the **Start** screen, click **Active Directory Administrative Center**. 2. In the console tree, click the arrow to expand **corp (local)**, and then click **Users**. 3. In the **Tasks** pane, click **New**, and then click **Group**. 4. In the Create Group dialog, type **DirectAccessClients** for Group name. 5. Scroll down to access the **Members** section of the Create Group dialog, and click **Add**. 6. Click **Object Types**, select **Computers**, and click **OK**. 7. Type **CLIENT1**, and then click **OK**. 8. Click **OK** to close the Create Group dialog. 9. Exit the Active Directory Administrative Center. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.    **New-ADGroup -GroupScope global -Name DirectAccessClients**  **Add-ADGroupMember -Identity DirectAccessClients -Members CLIENT1$** |

## Step 3: Configure EDGE1

EDGE1 configuration for the DirectAccess simplified deployment in an IPv4-only environment test lab consists of the following procedures:

* Install the Remote Access server role on EDGE1
* Deploy simplified DirectAccess using the Getting Started Wizard

The following sections explain these procedures in detail.

### Install the Remote Access server role on EDGE1

The Remote Access server role in Windows Server "8" Beta combines the DirectAccess feature and the RRAS role service into a new unified server role. This new Remote Access server role allows for centralized administration, configuration, and monitoring of both DirectAccess and VPN-based remote access services. Use the following procedure to install the Remote Access role on EDGE1.

To install the Remote Access server role on EDGE1

|  |
| --- |
| 1. In the **Dashboard** console of Server Manager, under **Configure this local server**, click **Add roles and features**. 2. Click **Next** three times to get to the server role selection screen. 3. In the **Select Server Roles** dialog, select **Remote Access**, click **Add Features** when prompted, and then click **Next**. 4. Click **Next** five times to accept the defaults for features, remote access role services, and web server role services. 5. On the Confirmation screen, click **Install**. 6. Wait for the feature installations to complete, and then click **Close**. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.    **Install-WindowsFeature RemoteAccess -IncludeManagementTools** |

### Deploy simplified DirectAccess using the Getting Started Wizard

The new Getting Started Wizard presents a greatly simplified configuration experience. The wizard masks the complexity of DirectAccess, and allows for an automated setup in a few simple steps. The wizard provides a seamless experience for the administrator by configuring Kerberos proxy automatically to eliminate the need for an internal PKI deployment. Use the following procedure to deploy simplified DirectAccess on EDGE1.

To configure DirectAccess using the Getting Started Wizard on EDGE1

|  |
| --- |
| 1. From the **Start** screen, click **Remote Access Management**. 2. In the Remote Access Management console, click **Run the Getting Started Wizard**. 3. Click **Deploy DirectAccess only**. 4. Verify that **Edge** is selected as the network topology. Type **edge1.contoso.com** as the public name to which remote access clients will connect. Click **Next**.   **Note:** By default, the Getting Started Wizard deploys DirectAccess to all laptops and notebook computers in the domain by applying a WMI filter to the client settings GPO. This default is not appropriate for the lab environment. Since the CLIENT1 PC is a member of the DirectAccessClients security group in Active Directory, take the following steps to change the client security group setting for DirectAccess.   1. On the final wizard page, click the link supplied to edit the wizard settings. 2. In the Remote Access Review dialog, next to **Remote Clients**, click **Change**. 3. On the Select Groups screen, clear the **Enable DirectAccess for mobile computers only** checkbox. 4. Click **Domain Computers (CORP\Domain Computers)**, and then click **Remove**. 5. Click **Add**, type **DirectAccessClients**, and then click **OK**. 6. Click **Next**, and then click **Finish**. 7. Click **OK** in the Remote Access Review screen, and then click **Finish**. 8. Since there is no PKI deployment in this test lab, the wizard will automatically provision self-signed certificates for IP-HTTPS and the Network Location Server, and will automatically enable Kerberos proxy. The wizard will also enable NAT64 and DNS64 for protocol translation in the IPv4-only environment. After the wizard successfully completes applying the configuration, click **Close**. 9. In the console tree of the Remote Access Management console, select **Operations Status**. Wait until the status of all monitors display as "Working". From the Tasks pane under Monitoring, click **Refresh** periodically to update the display. |

## Step 4: Configure CLIENT1

Use the following procedures to demonstrate remote access connectivity with CLIENT1:

* Connect CLIENT1 to the Corpnet subnet and update group policy
* Connect CLIENT1 to the Internet subnet and test remote access
* Connect CLIENT1 to the Homenet subnet and test remote access
* Monitor the client connection on the EDGE1 DirectAccess server

The following sections explain these procedures in detail.

### Connect CLIENT1 to the Corpnet subnet and update group policy

To receive the DirectAccess settings, CLIENT1 must update its group policy while connected to the Corpnet subnet.

To update group policy on CLIENT1 and apply DirectAccess settings

|  |
| --- |
| 1. Connect CLIENT1 to the Corpnet subnet. Reboot CLIENT1 while connected to the Corpnet subnet to update its security group membership and apply the DirectAccess client group policy settings. 2. From the Start screen, type **PowerShell**, then right-click **Windows PowerShell**, and click **Run as administrator**. 3. Type **Get-DnsClientNrptPolicy** and hit **ENTER**. The Name Resolution Policy Table (NRPT) entries for DirectAccess are displayed. Note that the NLS server exemption is displayed as DirectAccess-NLS.corp.contoso.com. The Getting Started wizard automatically created this DNS entry for the DirectAccess server, and provisioned an associated self-signed certificate so that the DirectAccess server can function as the Network Location Server. 4. Type **Get-NCSIPolicyConfiguration** and hit **ENTER**. The network connectivity status indicator settings deployed by the wizard are displayed. Note that the value of DomainLocationDeterminationURL is <https://DirectAccess-NLS.corp.contoso.com:443/insideoutside>. Whenever this network location server URL is accessible, the client will determine that it is inside the corporate network, and NRPT settings will not be applied. 5. Type **Get-DAConnectionStatus** and hit **ENTER**. Since the client can reach the network location server URL, the status will display as **ConnectedLocally**. |

### Connect CLIENT1 to the Internet subnet and test remote access

To test remote access connectivity from the Internet, move the CLIENT1 connection to the Internet subnet.

To test remote access from the Internet

|  |
| --- |
| 1. Connect CLIENT1 to the Internet subnet. Once the network determination process completes, the network icon should indicate Internet access. 2. In the PowerShell window, type **Get-DAConnectionStatus** and hit **ENTER**. The status should show as **ConnectedRemotely**. 3. Click the network icon in the System Notification Area. Note that **Workplace Connection** is listed as **Connected**. This is the default connection name provided by the DirectAccess wizard. 4. Right-click **Workplace Connection** and then click **Properties**. Note that Status shows as **Connected**. 5. From the PowerShell prompt, type **ping inet1.isp.example.com** and hit **ENTER** to verify Internet name resolution and connectivity. You should receive four replies from 131.107.0.1. 6. Type **ping app1.corp.contoso.com** and hit **ENTER** to verify corporate intranet name resolution and connectivity. Note the format of the IPv6 address returned. Since there is no IPv6 deployed in the test lab, the dynamically created NAT64 address of APP1 is returned. The dynamically created prefix assigned by DirectAccess for NAT64 will be in the form fdxx:xxxx:xxxx:7777::/96. 7. Click the Internet Explorer icon to launch IE. Verify that you can access the websites on **http://inet1.isp.example.com** and **http://app1.corp.contoso.com**. 8. From the desktop taskbar, click the **Windows Explorer** icon. 9. In the address bar, type **\\app1\Files**, and then press **ENTER**. 10. You should see a folder window with the contents of the Files shared folder. 11. In the **Files** shared folder window, double-click the **Example.txt** file. You should see the contents of the Example.txt file. 12. Close the **example.txt - Notepad** and the **Files** shared folder windows. 13. From the PowerShell window, type **Get-NetIPAddress** and then press **ENTER** to examine the client's IPv6 configuration. Note that the tunnel adapter iphttpsinterface is active with a valid IP-HTTPS address. CLIENT1 is using IP-HTTPS to tunnel IPv6 traffic to the EDGE1 server. 14. Type **Get-NetIPHTTPSConfiguration** and hit ENTER. Examine the settings applied by group policy to direct the client to https://edge1.contoso.com:443/IPHTTPS. 15. Type **wf.msc** and then hit **ENTER** to launch the Windows Firewall with Advanced Security console. Expand **Monitoring**, then **Security Associations** to examine the IPsec SAs established. Note that the authentication methods used are Computer Kerberos and User Kerberos, and that no certificate-based authentication was needed to establish the single tunnel simplified connection security rule. The client leverages the Kerberos proxy automatically deployed by the DirectAccess wizard. Select **Connection Security Rules** in the console tree to examine the associated policies applied. 16. Close the Windows Firewall with Advanced Security console. |

### Connect CLIENT1 to the Homenet subnet and test remote access

To test remote access connectivity from a simulated home network behind a NAT, move the CLIENT1 connection to the Homenet subnet.

To test remote access from the home network

|  |
| --- |
| 1. Connect CLIENT1 to the Homenet subnet. Once the network determination process completes, the network icon should indicate Internet access. 2. In the PowerShell window, type **Get-DAConnectionStatus** and hit **ENTER**. The status should show as **ConnectedRemotely**. 3. Click the network icon in the System Notification Area. Note that **Workplace Connection** is listed as **Connected**. Right-click **Workplace Connection** and then click **Properties**. Note that Status shows as **Connected**. 4. Type **ping app1.corp.contoso.com** and hit **ENTER** to verify corporate intranet name resolution and connectivity. Again, since there is no IPv6 deployed in the test lab, the dynamically created NAT64 address of APP1 is returned. 5. Click the Internet Explorer icon to launch IE. Verify that you can access the websites on **http://inet1.isp.example.com** and **http://app1.corp.contoso.com**. 6. Click **Start**, and then click the **Windows Explorer** icon. 7. In the address bar, type **\\app1\Files**, and then press **ENTER**. 8. You should see a folder window with the contents of the Files shared folder. 9. In the **Files** shared folder window, double-click the **Example.txt** file. You should see the contents of the Example.txt file. 10. Close the **example.txt - Notepad** and the **Files** shared folder windows. 11. From the PowerShell window, type **Get-NetIPAddress** and then press **ENTER** to examine the client's IPv6 configuration. Note that the tunnel adapter iphttpsinterface is active with a valid IP-HTTPS address. CLIENT1 is using IP-HTTPS to tunnel IPv6 traffic to the EDGE1 server. In previous versions of DirectAccess, a client with a private IPv4 address behind a NAT would connect using a Teredo IPv6 transition address. The simplified DirectAccess deployment wizard configures IP-HTTPS only. |

### Monitor the client connection on the EDGE1 DirectAccess server

The Remote Access Management Console in Windows Server "8" Beta provides remote client status monitoring functionality for both DirectAccess and VPN connections.

To monitor the client connection on EGDE1

|  |
| --- |
| 1. From the Start screen, click **Remote Access Management**. 2. In the Remote Access Management console, select **Dashboard**. 3. Examine the data collected under **Remote Client Status**. 4. In the Remote Access Management console, select **Remote Client Status**. 5. Double-click the CLIENT1 connection to display the detailed remote client statistics dialog. |

# Snapshot the Configuration

This completes the DirectAccess simplified deployment in an IPv4-only environment test lab. To save this configuration so that you can quickly return to a working Remote Access configuration from which you can test other Remote Access modular test lab guides (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 **DirectAccess simplified IPv4-only**. If your lab uses physical computers, create disk images to save the DirectAccess simplified IPv4-only test lab configuration.

# Additional Resources

For more information about DirectAccess, see the [DirectAccess TechNet portal page](http://technet.microsoft.com/en-us/network/dd420463.aspx).

For a list of all of the Windows Server "8" Beta TLGs, see [Windows Server "8" Beta Test Lab Guides](http://go.microsoft.com/fwlink/?LinkID=243062) in the TechNet Wiki.

For a list of additional Microsoft TLGs, see [Test Lab Guides](http://go.microsoft.com/fwlink/?LinkID=202817) in the TechNet Wiki.

To provide the authors of this guide with feedback or suggestions for improvement, send an email message to [tlgfb@microsoft.com](file:///C:\Users\josephd\Documents\SharePoint%20Drafts\tlgfb@microsoft.com).