



Windows Server® 2008 R2



Windows® 7

Step By Step Guide: Demonstrate DirectAccess in a Test Lab

Microsoft Corporation

Published: May 2009

Updated: October 2009

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). This paper contains an introduction to DirectAccess and instructions for setting up a test lab to demonstrate DirectAccess with a simulated Internet, intranet, and home network. For a short video describing this document, click [here](#).

Microsoft

Copyright Information

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release, and is the confidential and proprietary information of Microsoft Corporation.

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.

© 2009 Microsoft Corporation. All rights reserved.

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.....	7
In this guide.....	8
Scenario overview	9
Hardware and software requirements	10
Steps for configuring the test lab	11
Configure DC1	12
Install the operating system on DC1.....	13
Configure TCP/IP on DC1	13
Configure DC1 as a domain controller and DNS server	14
Install and configure DHCP	15
Create DNS A records	16
Install an enterprise root CA on DC1	16
Create a user account in Active Directory	17
Create a security group for DirectAccess client computers	18
Create and enable a custom certificate template	18
Create and enable firewall rules for ICMPv4 and ICMPv6 traffic.....	19
Remove ISATAP from the DNS global block list.....	22
Configure CRL distribution settings	22
Enable computer certificate auto-enrollment.....	23
Configure DA1	24
Install the operating system on DA1	24
Configure TCP/IP properties	24
Join DA1 to the CORP domain	26
Install the Web Server (IIS) role.....	27
Create a Web-based CRL distribution point	27
Configure permissions on the CRL distribution point file share	28
Publish the CRL on DA1	29
Obtain an additional certificate on DA1	29
Configure APP1	30
Install the operating system on APP1.....	31
Configure TCP/IP properties on APP1.....	31
Join APP1 to the CORP domain.....	32
Obtain an additional certificate on APP1	32
Install the Web Server (IIS) role.....	33
Configure the HTTPS security binding	33
Create a shared folder	34
Configure INET1	35

Install the operating system on INET1.....	35
Configure TCP/IP properties.....	35
Rename the computer.....	36
Install the Web Server (IIS) and DNS server roles.....	37
Create DNS A records.....	38
Install and configure DHCP.....	39
Configure NAT1.....	39
Install the operating system on NAT1.....	40
Configure Network Connections properties.....	40
Configure Internet Connection Sharing.....	41
Configure CLIENT1.....	41
Install the operating system on CLIENT1.....	42
User Account Control.....	42
Join CLIENT1 to the CORP domain.....	42
Add CLIENT1 to the DA_Clients security group.....	43
Verify the computer certificate on CLIENT1.....	43
Test access to intranet resources.....	44
Test access to the network location server.....	44
Test access to intranet resources from the Internet subnet.....	45
Configuring DirectAccess.....	45
Install the DirectAccess feature on DA1.....	46
Run the DirectAccess Setup wizard on DA1.....	46
Update IPv6 settings on APP1.....	47
Update IPv6 settings on DC1.....	48
Update Group Policy and IPv6 settings on CLIENT1.....	48
Verify ISATAP-based connectivity.....	48
Verifying DirectAccess functionality for CLIENT1 when connected to the Internet subnet.....	49
Connect CLIENT1 to the Internet subnet.....	49
Verify connectivity to Internet resources.....	50
Verify intranet access to Web and shared folder resources on APP1.....	50
Examine the CLIENT1 IPv6 configuration.....	51
Verifying DirectAccess functionality for CLIENT1 when connected to the Homenet subnet.....	51
Connect CLIENT1 to the Homenet subnet.....	52
Verify connectivity to Internet resources.....	52
Verify intranet access to Web and shared folder resources on APP1.....	52
Examine the CLIENT1 IPv6 configuration.....	53
Disable Teredo connectivity on CLIENT1.....	53
Verify intranet access to Web and file share resources on APP1.....	54
Enable Teredo connectivity on CLIENT1.....	54

Connect CLIENT1 to the Corpnet subnet.....	54
Additional Resources.....	55
Appendix.....	55
Set UAC behavior of the elevation prompt for administrators.....	56

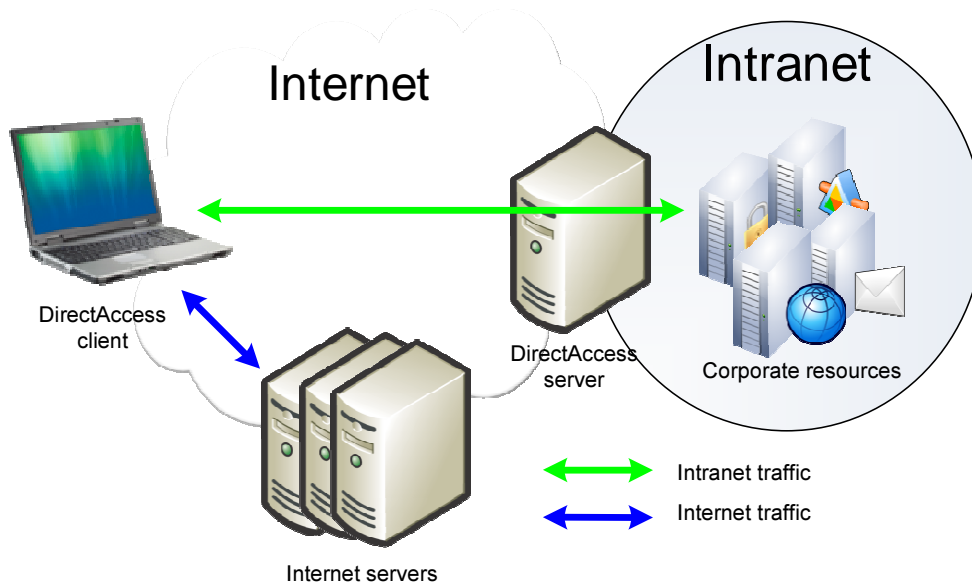
Introduction

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.

IT professionals can benefit from DirectAccess in many ways:

- **Improved Manageability of Remote Users.** Without DirectAccess, IT professionals can only manage mobile computers when users connect to a VPN or physically enter the office. With DirectAccess, IT professionals can manage mobile computers by updating Group Policy settings and distributing software updates any time the mobile computer has Internet connectivity, even if the user is not logged on. This flexibility allows IT professionals to manage remote computers on a regular basis and ensures that mobile users stay up-to-date with security and system health policies.
- **Secure and Flexible Network Infrastructure.** Taking advantage of technologies such as Internet Protocol version 6 (IPv6) and Internet Protocol security (IPsec), DirectAccess provides secure and flexible network infrastructure for enterprises. Below is a list of DirectAccess security and performance capabilities:
 - **Authentication.** DirectAccess authenticates the computer, enabling the computer to connect to the intranet before the user logs on. DirectAccess can also authenticate the user and supports two-factor authentication using smart cards.
 - **Encryption.** DirectAccess uses IPsec to provide encryption for communications across the Internet.
 - **Access Control.** IT professionals can configure which intranet resources different users can access using DirectAccess, granting DirectAccess users unlimited access to the intranet or only allowing them to use specific applications and access specific servers or subnets.
- **IT Simplification and Cost Reduction.** By default, DirectAccess separates intranet from Internet traffic, which reduces unnecessary traffic on the intranet by sending only traffic destined for the intranet through the DirectAccess server. Optionally, IT can configure DirectAccess clients to send all traffic through the DirectAccess server.

The following figure shows a DirectAccess client on the Internet.



In this guide

This paper contains instructions for setting up a test lab and deploying DirectAccess using four server computers, two client computers, Windows Server 2008 R2, and Windows 7. The 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 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 test lab configuration to a pilot or production deployment can result in configuration or functionality issues. For example, in this test lab configuration, you configure the DirectAccess server with static IPv4 addresses but no default gateways. In a pilot or production deployment on your intranet, you must configure a default gateway only on the Internet interface and static routes on the intranet interface. To ensure proper configuration and operation for your pilot or production DirectAccess deployment, use the information in the [DirectAccess Design Guide](#) for

planning and design decisions and the [DirectAccess Deployment Guide](#) for the steps to configure the DirectAccess server and supporting infrastructure servers.

Scenario overview

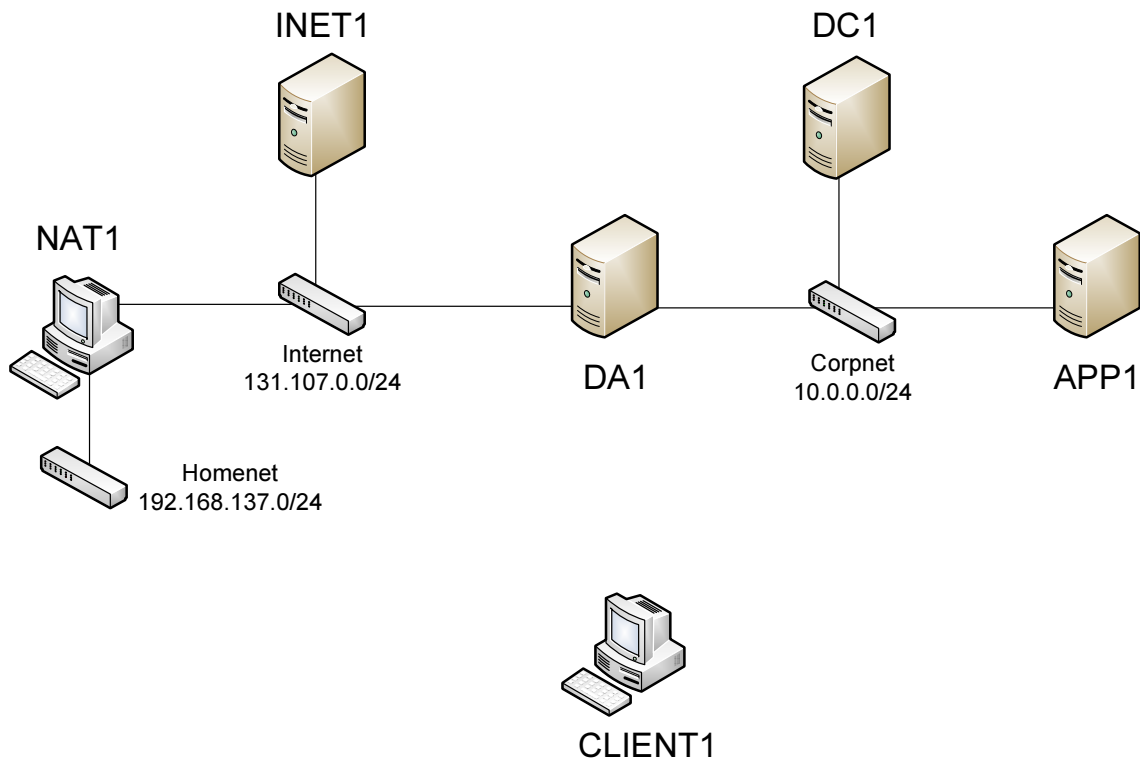
In this test lab, DirectAccess is deployed with:

- One computer running Windows Server 2008 R2 Standard 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 (DA1) that is configured as the DirectAccess server.
- One intranet member server running Windows Server 2008 R2 (APP1) that is configured as a general application server and network location server.
- One standalone server running Windows Server 2008 R2 (INET1) that is configured as an Internet DNS and Web server.
- One standalone client computer running Windows 7 (NAT1) that is configured as a network address translator (NAT) device using Internet Connection Sharing.
- One roaming member client computer running Windows 7 Enterprise Edition or 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 DirectAccess server.

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



CLIENT1 initially connects to the Corpnet subnet and joins the intranet domain. After DA1 is configured as a DirectAccess server and CLIENT1 is updated with the associated Group Policy settings, CLIENT1 connects to the Internet subnet and the Homenet subnet and tests DirectAccess connectivity to intranet resources on the Corpnet subnet.

Hardware and software requirements

The following are required components of the test lab:

- The product disc or files for Windows Server 2008 R2.
- The product disc or files for Windows 7.
- Four computers that meet the minimum hardware requirements for Windows Server 2008 R2. One of these computers has two network adapters installed.
- Two computers that meet the minimum hardware requirements for Windows 7. One of these computers has two network adapters installed.

Note If you are using operating system images for test lab computers, you must use images prepared with the System Preparation (Sysprep) tool. Due to the security requirements of DirectAccess connections, you cannot use cloned images.

Steps for configuring the test lab

There are six steps to follow when setting up this test lab.

1. Configure DC1.

DC1 is a server computer running Windows Server 2008 R2 Standard Edition. DC1 is configured as a domain controller with Active Directory and acts as the DNS and DHCP server for the intranet subnet. DC1 also serves as an enterprise root CA for the domain.

2. Configure DA1.

DA1 is a member server computer running Windows Server 2008 R2. DA1 is configured with Internet Information Services (IIS). After the setup of the test lab, DA1 will be configured as a DirectAccess server.

3. Configure APP1.

APP1 is a member server computer running Windows Server 2008 R2. APP1 is configured with IIS and also acts as a file server.

4. Configure INET1.

INET1 is a standalone server computer running Windows Server 2008 R2. INET1 is configured as an Internet DNS and Web server.

5. Configure NAT1.

NAT1 is a client computer running Windows 7. NAT1 is configured as a NAT device on the edge of the Homenet subnet, simulating routers that are used in many homes to connect multiple computers to the Internet.

6. Configure CLIENT1.

CLIENT1 is a client computer running Windows 7. CLIENT1 is configured as a DirectAccess client.



Note

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

After the individual server and client computers are configured, this guide provides steps for configuring the DirectAccess server and client and demonstrating DirectAccess connectivity from the Internet and Homenet subnets. The following sections provide details about how to perform these tasks.

Configure DC1

DC1 is a computer running Windows Server 2008 R2 Standard Edition and providing the following services:

- A domain controller for the corp.contoso.com Active Directory Domain Services (AD DS) domain.
- A DNS server for the corp.contoso.com DNS domain.
- A DHCP server for the Corpnet subnet.
- An enterprise root CA for the corp.contoso.com domain.

DC1 configuration consists of the following steps:

- Install the operating system.
- Configure TCP/IP.
- Install Active Directory and DNS.
- Install DHCP.
- Create DNS records.
- Install an enterprise root CA.
- Create a user account in Active Directory.
- Create a DirectAccess client security group.
- Create a custom certificate template.
- Configure firewall rules for Internet Control Message Protocol for IPv4 (ICMPv4) and ICMP for IPv6 (ICMPv6) traffic.
- Remove ISATAP from the DNS global block list.
- Configure certificate revocation list (CRL) distribution settings.

- Enable computer certificate auto-enrollment.

The following sections explain these steps in detail.

Install the operating system on DC1

First, install Windows Server 2008 R2 Standard Edition as a standalone server.

▶ To install the operating system on DC1

1. Start the installation of Windows Server 2008 R2.
2. Follow the instructions to complete the installation, specifying Windows Server 2008 R2 Standard Edition and a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect the network adapter to the Corpnet subnet.

Configure TCP/IP on DC1

Next, configure the TCP/IP protocol with a static IP address of 10.0.0.1 and the subnet mask of 255.255.255.0.

▶ To configure TCP/IP on DC1

1. In **Initial Configuration Tasks**, click **Configure networking**.
2. In **Network Connections**, right-click **Local Area Connection**, and then click **Properties**.
3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
4. Select **Use the following IP address**, type **10.0.0.1** next to **IP address**, and type **255.255.255.0** next to **Subnet mask**.
5. Click **Advanced**, and then click the **DNS** tab.
6. In **DNS suffix for this connection**, type **corp.contoso.com**, click **OK** twice, and then click **Close**.
7. Close the **Network Connections** window.
8. In **Initial Configuration Tasks**, click **Provide computer name and domain**.
9. In **System Properties**, click **Change**. In **Computer name**, type **DC1**, and click **OK** twice, and then click **Close**. When you are prompted to restart the computer, click **Restart**

Now.

10. After restarting, login using the local administrator account.
11. In **Initial Configuration Tasks**, click **Do not show this window at logon**, and then click **Close**.

Configure DC1 as a domain controller and DNS server

Next, configure DC1 as a domain controller and DNS server for the corp.contoso.com domain.

To configure DC1 as a domain controller and DNS server

1. In the console tree of **Server Manager**, click **Roles**. In the details pane, click **Add Roles**, and then click **Next**.
2. On the **Select Server Roles** page, click **Active Directory Domain Services**, click **Add Required Features**, click **Next** twice, and then click **Install**. When installation is complete, click **Close**.
3. To start the Active Directory Installation Wizard, click **Start**, type **dcpromo**, and then press ENTER.
4. In the **Active Directory Installation Wizard** dialog box, click **Next** twice.
5. On the **Choose a Deployment Configuration** page, click **Create a new domain in a new forest**, and then click **Next**.
6. On the **Name the Forest Root Domain** page, type **corp.contoso.com**, and then click **Next**.
7. On the **Set Forest Functional Level** page, in **Forest Functional Level**, click **Windows Server 2008 R2**, and then click **Next**.
8. On the **Additional Domain Controller Options** page, click **Next**, click **Yes** to continue, and then click **Next**.
9. On the **Directory Services Restore Mode Administrator Password** page, type a strong password twice, and then click **Next**.
10. On the **Summary** page, click **Next**.
11. Wait while the wizard completes the configuration of Active Directory and DNS services, and then click **Finish**.

12. When you are prompted to restart the computer, click **Restart Now**.
13. After the computer restarts, log in to the CORP domain using the Administrator account.

Install and configure DHCP

Next, configure DC1 as a DHCP server so that CLIENT1 can automatically configure itself when connecting to the Corpnet subnet.

▶ To install and configure the DHCP server role on DC1

1. In the console tree of **Server Manager**, click **Roles**.
2. In the details pane, under **Roles Summary**, click **Add roles**, and then click **Next**.
3. On the **Select Server Roles** page, click **DHCP Server**, and then click **Next** twice.
4. On the **Select Network Connection Bindings** page, verify that **10.0.0.1** is selected, and then click **Next**.
5. On the **Specify IPv4 DNS Server Settings** page, verify that **corp.contoso.com** is listed under **Parent domain**.
6. Type **10.0.0.1** under **Preferred DNS server IP address**, and click **Validate**. Verify that the result returned is **Valid**, and then click **Next**.
7. On the **Specify WINS Server Settings** page, accept the default setting of **WINS is not required on this network**, and then click **Next**.
8. On the **Add or Edit DHCP Scopes** page, click **Add**.
9. In the **Add Scope** dialog box, type **Corpnet** next to **Scope Name**. Next to **Starting IP Address**, type **10.0.0.100**, next to **Ending IP Address**, type **10.0.0.150**, and next to **Subnet Mask**, type **255.255.255.0**. Click **OK**, and then click **Next**.
10. On the **Configure DHCPv6 Stateless Mode** page, select **Disable DHCPv6 stateless mode for this server**, and then click **Next**.
11. On the **Authorize DHCP Server** page, select **Use current credentials**. Verify that **CORP\Administrator** is displayed next to **User Name**, and then click **Next**.
12. On the **Confirm Installation Selections** page, click **Install**.
13. Verify the installation was successful, and then click **Close**.

Create DNS A records

Next, create DNS Address (A) records for the names `crl.contoso.com` and `nls.corp.contoso.com`.

▶ To create DNS A records

1. Click **Start**, point to **Administrative Tools**, and then click **DNS**.
2. In the console tree of DNS Manager, open **DC1**.
3. Right-click **Forward Lookup Zones**, click **New Zone**, and then click **Next**.
4. On the **Zone Type** page, click **Next**.
5. On the **Active Directory Zone Replication** page, click **Next**.
6. On the **Zone Name** page, type `contoso.com`, and then click **Next**.
7. On the **Dynamic Update** page, click **Allow both nonsecure and secure dynamic updates**, click **Next**, and then click **Finish**.
8. In the console tree, right click `contoso.com`, and then click **New Host (A or AAAA)**.
9. In **Name**, type `crl`. In **IP address**, type `10.0.0.2`. Click **Add Host**, click **OK**, and then click **Done**.
10. In the console tree, open `corp.contoso.com`.
11. Right click `corp.contoso.com`, and then click **New Host (A or AAAA)**.
12. In **Name**, type `nls`. In **IP address**, type `10.0.0.3`. Click **Add Host**, click **OK**, and then click **Done**.
13. Close the DNS Manager console.

Install an enterprise root CA on DC1

Protected communication across the Internet between DirectAccess clients and servers requires computer certificates for IPsec-based authentication. In this step, install an enterprise root CA on DC1 to provide computer certificates for domain member computers.

▶ To install an enterprise root CA on DC1

1. In the console tree of **Server Manager**, click **Roles**.
2. Under **Roles Summary**, click **Add roles**, and then click **Next**.

3. On the **Select Server Roles** page, click **Active Directory Certificate Services**, and then click **Next** twice.
4. On the **Role Services** page, click **Next**.
5. On the **Setup Type** page, click **Enterprise**, and then click **Next**.
6. On the **CA Type** page, click **Root CA**, and then click **Next**.
7. On the **Private Key** page, click **Create a new private key**, and then click **Next**.
8. On the **Cryptography** page, click **Next**.
9. On the **CA Name** page, click **Next**.
10. On the **Validity Period** page, click **Next**.
11. On the **Certificate Database** page, click **Next**.
12. On the **Confirm Installation Selections** page, click **Install**.
13. On the **Results** page, click **Close**.

Create a user account in Active Directory

Next, create a user account in Active Directory that will be used when logging in to CORP domain member computers.

To create a user account in Active Directory

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, open **corp.contoso.com**, right-click **Users**, point to **New**, and then click **User**.
3. In the **New Object - User** dialog box, next to **Full name**, type **User1 User**, and in **User logon name**, type **User1**.
4. Click **Next**.
5. In **Password**, type the password that you want to use for this account, and in **Confirm password**, type the password again.
6. Clear the **User must change password at next logon** check box, and select the **Password**

never expires check box.

7. Click **Next**, and then click **Finish**.
8. In the console tree, click **Users**.
9. In the details pane, double-click **Domain Admins**.
10. In the **Domain Admins Properties** dialog box, click the **Members** tab, and then click **Add**.
11. Under **Enter the object names to select (examples)**, type **User1**, and then click **OK** twice.
12. Leave the Active Directory Users and Computers console open for the following procedure.

Create a security group for DirectAccess client computers

Next, create a security group that will be used to apply DirectAccess client computer settings to the member computers. The CLIENT1 computer account will be added to this security group after joining the domain.

To create a security group for DirectAccess client computers

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

Create and enable a custom certificate template

Next, create a certificate template so that requesting computers can specify the subject name and subject alternative name of a certificate.

To create and enable a custom certificate template

1. Click **Start**, type **mmc**, and then press ENTER.
2. Click **File**, and then click **Add/Remove Snap-in**.

3. In the list of snap-in, click Certificate Templates, click **Add**, and then click **OK**.
4. In the console tree, open **Certificates Templates**.
5. In the contents pane, right-click the **Web Server** template, and then click **Duplicate Template**.
6. Click **Windows Server 2008 Enterprise**, and then click **OK**.
7. In **Template display name**, type **Web Server 2008**.
8. Click the **Security** tab.
9. Click **Authenticated Users**, and then select **Enroll** in the **Allow** column.
10. Click **Add**, type **Domain Computers**, and then click **OK**.
11. Click **Domain Computers**, and then select **Enroll** in the **Allow** column.
12. Click the **Request Handling** tab.
13. Select **Allow private key to be exported**.
14. Click **OK**.
15. Close the MMC window without saving changes.
16. Click **Start**, point to **Administrative Tools**, and then click **Certification Authority**.
17. In the console tree, expand **corp-DC1-CA**, right-click **Certificate Templates**, point to **New**, and then click **Certificate Template To Issue**.
18. In the list of certificate templates, click **Web Server 2008**, and then click **OK**.
19. Close the Certification Authority console.

Create and enable firewall rules for ICMPv4 and ICMPv6 traffic

Next, configure Windows Firewall with Advanced Security rules that allow inbound and outbound ICMPv4 and ICMPv6 Echo Request messages. These messages need to be sent and received to provide connectivity for Teredo-based DirectAccess clients.

To create and enable firewall rules for ICMPv4 and ICMPv6 traffic

1. Click **Start**, click **Administrative Tools**, and then click **Group Policy Management**.

2. In the console tree, open **Forest: Contoso.com\Domains\corp.contoso.com**.
3. In the console tree, right-click **Default Domain Policy**, and then click **Edit**.
4. In the console tree of the Group Policy Management Editor, open **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security**.
5. In the console tree, right-click **Inbound Rules**, and then click **New Rule**.
6. On the Rule Type page, click **Custom**, and then click **Next**.
7. On the Program page, click **Next**.
8. On the Protocols and Ports page, for **Protocol type**, click **ICMPv4**, and then click **Customize**.
9. In the **Customize ICMP Settings** dialog box, click **Specific ICMP types**, select **Echo Request**, and then click **OK**.
10. Click **Next**.
11. On the Scope page, click **Next**.
12. On the Action page, click **Next**.
13. On the Profile page, click **Next**.
14. On the Name page, for **Name**, type **Inbound ICMPv4 Echo Requests**, and then click **Finish**.
15. In the console tree, right-click **Inbound Rules**, and then click **New Rule**.
16. On the Rule Type page, click **Custom**, and then click **Next**.
17. On the Program page, click **Next**.
18. On the Protocols and Ports page, for **Protocol type**, click **ICMPv6**, and then click **Customize**.
19. In the **Customize ICMP Settings** dialog box, click **Specific ICMP types**, select **Echo Request**, and then click **OK**.
20. Click **Next**.

21. On the Scope page, click **Next**.
22. On the Action page, click **Next**.
23. On the Profile page, click **Next**.
24. On the Name page, for **Name**, type **Inbound ICMPv6 Echo Requests**, and then click **Finish**.
25. In the console tree, right-click **Outbound Rules**, and then click **New Rule**.
26. On the Rule Type page, click **Custom**, and then click **Next**.
27. On the Program page, click **Next**.
28. On the Protocols and Ports page, for **Protocol type**, click **ICMPv4**, and then click **Customize**.
29. In the **Customize ICMP Settings** dialog box, click **Specific ICMP types**, select **Echo Request**, and then click **OK**.
30. Click **Next**.
31. On the Scope page, click **Next**.
32. On the Action page, click **Allow the connection**, and then click **Next**.
33. On the Profile page, click **Next**.
34. On the Name page, for **Name**, type **Outbound ICMPv4 Echo Requests**, and then click **Finish**.
35. In the console tree, right-click **Outbound Rules**, and then click **New Rule**.
36. On the Rule Type page, click **Custom**, and then click **Next**.
37. On the Program page, click **Next**.
38. On the Protocols and Ports page, for **Protocol type**, click **ICMPv6**, and then click **Customize**.
39. In the **Customize ICMP Settings** dialog box, click **Specific ICMP types**, select **Echo Request**, and then click **OK**.
40. Click **Next**.

41. On the Scope page, click **Next**.
42. On the Action page, click **Allow the connection**, and then click **Next**.
43. On the Profile page, click **Next**.
44. On the Name page, for **Name**, type **Outbound ICMPv6 Echo Requests**, and then click **Finish**.
45. Close the Group Policy Management Editor and Group Policy Management consoles.

Remove ISATAP from the DNS global block list

Next, configure the DNS Server service to remove the ISATAP name from its default global block list.

To remove ISATAP from the DNS global query block list

1. Click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
2. In the Command Prompt window, type **dnscmd /config /globalqueryblocklist wpad**, and then press ENTER.
3. Close the Command Prompt window.

Configure CRL distribution settings

Next, configure the enterprise root CA with additional CRL distribution settings so that DirectAccess clients can check the CRL of certificates when connected to any of the test lab subnets.

To configure additional CRL distribution settings

1. Click **Start**, point to **Administrative Tools**, and then click **Certification Authority**.
2. In the console tree, right-click **corp-DC1-CA**, and then click **Properties**.
3. Click the **Extensions** tab, and then click **Add**.
4. In **Location**, type **http://crl.contoso.com/crld/**.
5. In **Variable**, click **<CAName>**, and then click **Insert**.
6. In **Variable**, click **<CRLNameSuffix>**, and then click **Insert**.

7. In **Variable**, click **<DeltaCRLAllowed>**, and then click **Insert**.
8. In **Location**, type **.crl** at the end of the Location string, and then click **OK**.
9. Select **Include in CRLs. Clients use this to find Delta CRL locations.** and **Include in the CDP extension of issued certificates**, and then click **OK**.
10. Click **Add**.
11. In **Location**, type **\\da1\crl-dist**.
12. In **Variable**, click **<CAName>**, and then click **Insert**.
13. In **Variable**, click **<CRLNameSuffix>**, and then click **Insert**.
14. In **Variable**, click **<DeltaCRLAllowed>**, and then click **Insert**.
15. In **Location**, type **.crl** at the end of the string, and then click **OK**.
16. Select **Publish CRLs to this location** and **Publish Delta CRLs to this location**, and then click **OK**.
17. Click **Yes** to restart Active Directory Certificate Services.
18. Close the Certification Authority console.

Enable computer certificate auto-enrollment

Next, configure the root CA so that computer certificates are issued automatically through Group Policy.

To configure computer certificate auto-enrollment

1. Click **Start**, click **Administrative Tools**, and then click **Group Policy Management**.
2. In the console tree, open **Forest: corp.contoso.com\Domains\corp.contoso.com**.
3. In the console tree, right-click **Default Domain Policy**, and then click **Edit**.
4. In the console tree of the Group Policy Management Editor, open **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies**.
5. In the details pane, right-click **Automatic Certificate Request Settings**, point to **New**, and then click **Automatic Certificate Request**.

6. In the Automatic Certificate Request Wizard, click **Next**.
7. On the **Certificate Template** page, click **Computer**, click **Next**, and then click **Finish**.
8. Close the Group Policy Management Editor and Group Policy Management consoles.

Configure DA1

DA1 will run Windows Server 2008 R2 and it will host the IIS role. DA1 configuration consists of the following steps:

- Install the operating system.
- Configure TCP/IP.
- Join the computer to the domain.
- Install the Web Server (IIS) role.
- Create a Web-based CRL distribution point.
- Configure permissions on the CRL distribution point file share.
- Publish the CRL on DA1.
- Obtain an additional certificate

DA1 must have two network adapters installed.

Install the operating system on DA1

First, install Windows Server 2008 R2 as a standalone server.

To install the operating system on DA1

1. Start the installation of Windows Server 2008 R2.
2. Follow the instructions to complete the installation, specifying a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect one network adapter to the Corpnet subnet and the other to the Internet subnet.

Configure TCP/IP properties

Configure the TCP/IP protocol with static IP addresses on both interfaces.

▶ **To configure TCP/IP properties on the Corpnet adapter**

1. In **Initial Configuration Tasks**, click **Configure networking**.
2. In **Network Connections**, right-click the network connection that is connected to the Corpnet subnet, and then click **Rename**.
3. Type **Corpnet**, and then press ENTER.
4. Right-click **Corpnet**, and then click **Properties**.
5. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
6. Select **Use the following IP address**. In **IP address**, type **10.0.0.2**. In **Subnet mask**, type **255.255.255.0**.
7. Select **Use the following DNS server addresses**. In **Preferred DNS server**, type **10.0.0.1**.
8. Click **Advanced**, and then the **DNS** tab.
9. In **DNS suffix for this connection**, type **corp.contoso.com**, click **OK** twice, and then click **Close**.
10. In the **Network Connections** window, right-click the network connection that is connected to the Internet subnet, and then click **Rename**.
11. Type **Internet**, and then press ENTER.
12. Right-click **Internet**, and then click **Properties**.
13. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
14. Select **Use the following IP address**. In **IP address**, type **131.107.0.2**. In **Subnet mask**, type **255.255.255.0**.
15. Click **Advanced**. On the **IP Settings** tab, click **Add** for **IP Addresses**.
16. In **IP address**, type **131.107.0.3**. In **Subnet mask**, type **255.255.255.0**, and then click **Add**.
17. Click the **DNS** tab.
18. In **DNS suffix for this connection**, type **isp.example.com**, and then click **OK** three times.
19. Close the Network Connections window.

20. To check network communication between DA1 and DC1, click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**.
21. In the Command Prompt window, type **ping dc1.corp.contoso.com**.
22. Verify that there are four responses from 10.0.0.1.
23. Close the Command Prompt window.

Note

You need to configure two consecutive public IPv4 addresses on the DirectAccess server's Internet interface so that Teredo-based DirectAccess clients can detect the type of NAT that they are located behind (cone vs. symmetric). For more information, see [Teredo Overview](#).

Join DA1 to the CORP domain

▶ To join DA1 to the CORP domain

1. In **Initial Configuration Tasks**, click **Provide Computer Name and Domain**.
2. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
3. In **Computer Name**, type **DA1**. In **Member of**, click **Domain**, and then type **corp.contoso.com**.
4. Click **OK**.
5. When you are prompted for a user name and password, type **User1** and its password, and then click **OK**.
6. When you see a dialog box welcoming you to the corp.contoso.com domain, click **OK**.
7. When you are prompted that you must restart the computer, click **OK**.
8. On the **System Properties** dialog box, click **Close**.
9. When you are prompted to restart the computer, click **Restart Now**.
10. After the computer has restarted, click **Switch User**, and then click **Other User** and log on to the CORP domain with the **User1** account.
11. In **Initial Configuration Tasks**, click **Do not show this window at logon**, and then click **Close**.

Install the Web Server (IIS) role

Next, install the Web Server (IIS) role to make DA1 a Web server. DA1 will host an external CRL so that remote DirectAccess clients can access a Web-based CRL distribution point for IP-HTTPS-based connections.

▶ To install the IIS server role

1. In the console tree of **Server Manager**, click **Roles**. In the details pane, click **Add Roles**, and then click **Next**.
2. On the **Select Server Roles** page, click **Web Server (IIS)**, and then click **Next** three times.
3. Click **Install**.
4. Verify that all installations were successful, and then click **Close**.
5. Leave the Server Manager window open.

Create a Web-based CRL distribution point

Next, create a Web-based CRL distribution point for DirectAccess clients.

▶ To create a Web-based CRL distribution point

1. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the console tree, open **DA1**, and then **Sites**.
3. Right-click **Default Web Site**, and then click **Add virtual directory**.
4. In **Alias**, type **CRLD**.
5. In **Physical path**, click the ellipsis (...).
6. Click the drive on which Windows Server 2008 R2 is located, and then click **Make New Folder**.
7. Type **CRLDist**, press ENTER, and then click **OK** twice.
8. In the contents pane, double-click **Directory Browsing**.
9. In the **Actions** pane, click **Enable**.
10. In the console tree, click the **CRLD** folder.

11. In the contents pane, double-click **Configuration Editor**.
12. In **Section**, open **system.webServer\security\authentication\requestFiltering**.
13. In the contents pane, double-click **allowDoubleEscaping** to change it from **False** to **True**.
14. In the **Actions** pane, click **Apply**.
15. Close the Internet Information Services (IIS) Manager window.

Configure permissions on the CRL distribution point file share

Next, configure the permissions on the CRLDist file share so that DC1 can write the CRL files.

To configure permissions on the CRLDist file share

1. Click **Start**, and then click **Computer**.
2. Double-click the drive on which Windows Server 2008 R2 is located.
3. In the details pane, right-click the **CRLDist** folder, and then click **Properties**.
4. Click the **Sharing** tab, and then click **Advanced Sharing**.
5. Select **Share this folder**.
6. In **Share name**, add **\$** to the end of the CRLDist name to hide the share, and then click **Permissions**.
7. Click **Add**, and then click **Object Types**.
8. Select **Computers**, and then click **OK**.
9. In **Enter the object names to select**, type **DC1**, and then click **OK**.
10. In **Group or user names**, click the **DC1** computer. In **Permissions for DC1**, click **Full Control**, and then click **OK** twice.
11. Click the **Security** tab, and then click **Edit**.
12. Click **Add**, and then click **Object Types**.
13. Select **Computers**, and then click **OK**.
14. In **Enter the object names to select**, type **DC1**, and then click **OK**.
15. In **Group or user names**, click the **DC1** computer. In **Permissions for DC1**, click **Full**

Control, click **OK**, and then click **Close**.

16. Close the **Local Disk** window.

Publish the CRL on DA1

Next, publish the CRL from DC1 and check for CRL files on DA1.

To publish the CRL

1. On DC1, click **Start**, point to **Administrative Tools**, and then click **Certification Authority**.
2. In the console tree, double-click **corp-DC1-CA**, right-click **Revoked Certificates**, point to **All Tasks**, and then click **Publish**.
3. If prompted, click **New CRL**, and then click **OK**.
4. Click **Start**, type `\\da1\crl-dist$`, and then press ENTER.
5. In the `crl-dist$` window, you should see two CRL files named **corp-DC1-CA** and **corp-DC1-CA+**.
6. Close the `crl-dist$` window and the Certification Authority console.

Obtain an additional certificate on DA1

Next, obtain an additional certificate for DA1 with a customized subject and alternative name for IP-HTTPS connectivity.

To obtain an additional certificate for DA1

1. On DA1, click **Start**, type `mmc`, and then press ENTER. Click Yes at the User Account Control prompt.
2. Click **File**, and then click **Add/Remove Snap-ins**.
3. Click **Certificates**, click **Add**, click **Computer account**, click **Next**, select **Local computer**, click **Finish**, and then click **OK**.
4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**.
5. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.
6. Click **Next** twice.

7. On the Request Certificates page, click **Web Server 2008**, and then click **More information is required to enroll for this certificate**.
8. On the **Subject** tab of the **Certificate Properties** dialog box, in **Subject name**, for **Type**, select **Common Name**.
9. In **Value**, type **da1.contoso.com**, and then click **Add**.
10. In **Alternative name**, for **Type**, select **DNS**.
11. In **Value**, type **da1.contoso.com**, and then click **Add**.
12. Click **OK**, click **Enroll**, and then click **Finish**.
13. In the details pane of the Certificates snap-in, verify that a new certificate with the name da1.contoso.com was enrolled with **Intended Purposes** of **Server Authentication**.
14. Right-click the certificate, and then click **Properties**.
15. In **Friendly Name**, type **IP-HTTPS Certificate**, and then click **OK**.
16. Close the console window. If you are prompted to save settings, click **No**.

Configure APP1

APP1 will run Windows Server 2008 R2, host the IIS role, and act as the network location server. APP1 configuration consists of the following steps:

- Install the operating system.
- Configure TCP/IP.
- Join the computer to the domain.
- Obtain an additional certificate.
- Install the Web Server (IIS) role.
- Configure the HTTPS security binding.
- Create a shared folder.

Install the operating system on APP1

▶ To install the operating system on APP1

1. Start the installation of Windows Server 2008 R2.
2. Follow the instructions to complete the installation, specifying a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect the network adapter to the Corpnet subnet.

Configure TCP/IP properties on APP1

▶ To configure TCP/IP properties on APP1

1. In **Initial Configuration Tasks**, click **Configure networking**.
2. In the **Network Connections** window, right-click **Local Area Connection**, and then click **Properties**.
3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
4. Select **Use the following IP address**. In **IP address**, type **10.0.0.3**. In **Subnet mask**, type **255.255.255.0**.
5. Select **Use the following DNS server addresses**. In **Preferred DNS server**, type **10.0.0.1**.
6. Click **Advanced**, and then click the **DNS** tab. In **DNS suffix for this connection**, type **corp.contoso.com**, click **OK** twice, and then click **Close**.
7. Close the **Network Connections** window and leave the **Initial Configuration Tasks** window open.
8. To check name resolution and network communication between APP1 and DC1, click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**.
9. In the Command Prompt window, type **ping dc1.corp.contoso.com**.
10. Verify that there are four replies from 10.0.0.1.
11. Close the Command Prompt window.

Join APP1 to the CORP domain

▶ To join APP1 to the CORP domain

1. In **Initial Configuration Tasks**, click **Provide Computer Name and Domain**.
2. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
3. In **Computer Name**, type **APP1**. In **Member of**, click **Domain**, and then type **corp.contoso.com**.
4. Click **OK**.
5. When you are prompted for a user name and password, type **User1** and its password, and then click **OK**.
6. When you see a dialog box welcoming you to the corp.contoso.com domain, click **OK**.
7. When you are prompted that you must restart the computer, click **OK**.
8. On the **System Properties** dialog box, click **Close**.
9. When you are prompted to restart the computer, click **Restart Now**.
10. After the computer restarts, click **Switch User**, and then click **Other User** and log on to the CORP domain with the **User1** account.
11. In **Initial Configuration Tasks**, click **Do not show this window at logon**, and then click **Close**.

Obtain an additional certificate on APP1

Next, obtain an additional certificate for APP1 with a customized subject and alternative name for network location.

▶ To obtain an additional certificate for APP1

1. Click **Start**, type **mmc**, and then press ENTER.
2. Click **File**, and then click **Add/Remove Snap-in**.
3. Click **Certificates**, click **Add**, select **Computer account**, click **Next**, select **Local computer**, click **Finish**, and then click **OK**.
4. In the console tree of the Certificates snap-in, open **Certificates (Local**

Computer)\Personal\Certificates.

5. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.
6. Click **Next** twice.
7. On the **Request Certificates** page, click **Web Server 2008**, and then click **More information is required to enroll for this certificate**.
8. On the **Subject** tab of the **Certificate Properties** dialog box, in **Subject name**, for **Type**, select **Common Name**.
9. In **Value**, type **nls.corp.contoso.com**, and then click **Add**.
10. In **Alternative name**, for **Type**, select **DNS**.
11. In **Value**, type **nls.corp.contoso.com**, and then click **Add**.
12. Click **OK**, click **Enroll**, and then click **Finish**.
13. In the details pane of the Certificates snap-in, verify that a new certificate with the name **nls.corp.contoso.com** was enrolled with **Intended Purposes of Server Authentication**.
14. Close the console window. If you are prompted to save settings, click **No**.

Install the Web Server (IIS) role

Next, install the Web Server (IIS) role to make APP1 a Web server.

To install the Web Server (IIS) server role

1. In the console tree of **Server Manager**, click **Roles**. In the details pane, click **Add Roles**, and then click **Next**.
2. On the **Select Server Roles** page, select the **Web Server (IIS)** check box, and then click **Next** three times.
3. Click **Install**.
4. Verify that all installations were successful, and then click **Close**.

Configure the HTTPS security binding

Next, configure the HTTPS security binding so that APP1 can act as the network location server.

▶ **To configure the HTTPS security binding**

1. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the console tree of Internet Information Services (IIS) Manager, open **APP1/Sites**, and then click **Default Web site**.
3. In the **Actions** pane, click **Bindings**.
4. In the **Site Bindings** dialog box, click **Add**.
5. In the **Add Site Binding** dialog box, in the **Type** list, click **https**. In **SSL Certificate**, click the certificate with the name **nls.corp.contoso.com**. Click **OK**, and then click **Close**.
6. Close the Internet Information Services (IIS) Manager console.

Create a shared folder

Next, create a shared folder and a text file within the folder.

▶ **To create a shared folder**

1. Click **Start**, and then click **Computer**.
2. Double-click the drive on which Windows Server 2008 R2 is installed.
3. Click **New Folder**, type **Files**, and then press ENTER. Leave the **Local Disk** window open.
4. Click **Start**, click **All Programs**, click **Accessories**, right-click **Notepad**, and then click **Run as administrator**.
5. In the **Untitled – Notepad** window, type **This is a shared file**.
6. Click **File**, click **Save**, double-click **Computer**, double-click the drive on which Windows Server 2008 R2 is installed, and then double-click the **Files** folder.
7. In **File name**, type **Example.txt**, and then click **Save**. Close the Notepad window.
8. In the **Local Disk** window, right-click the **Files** folder, point to **Share with**, and then click **Specific people**.
9. Click **Share**, and then click **Done**.
10. Close the **Local Disk** window.

Configure INET1

INET1 will run Windows Server 2008 R2 and it will host the Web Server (IIS), DNS, and DHCP server roles. INET1 configuration consists of the following steps:

- Install the operating system.
- Configure TCP/IP.
- Rename the computer.
- Install the Web Server (IIS) and DNS server roles.
- Install DHCP.
- Create DNS records.

Install the operating system on INET1

To install the operating system on INET1

1. Start the installation of Windows Server 2008 R2.
2. Follow the instructions to complete the installation, specifying a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect the network adapter of INET1 to the Internet subnet.

Configure TCP/IP properties

To configure TCP/IP properties

1. In **Initial Configuration Tasks**, click **Configure networking**.
2. In the **Network Connections** window, right-click **Local Area Connection**, and then click **Properties**.
3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
4. Select **Use the following IP address**. In **IP address**, type **131.107.0.1**. In **Subnet mask**, type **255.255.255.0**.
5. Click **Advanced**, and then click the **DNS** tab.
6. In **DNS suffix for this connection**, type **isp.example.com**, and then click **OK**.

7. Click **OK**, and then click **Close** to close the **Local Area Connection Properties** dialog box.
8. Close the **Network Connections** window.
9. To check network communication between INET1 and DA1, click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**.
10. In the Command Prompt window, type **ping 131.107.0.2**.
11. Verify that there are four responses from 131.107.0.2.
12. Close the Command Prompt window.
13. Click **Start**, right-click **Network**, and then click **Properties**.
14. In the **Network and Sharing Center** window, click **Change advanced sharing settings**.
15. In the **Advanced sharing settings** window, click **Turn on file and printer sharing**, and then click **Save changes**.
16. Close the **Network and Sharing Center** window.

Rename the computer

▶ To rename the computer to INET1

1. In **Initial Configuration Tasks**, click **Provide Computer Name and Domain**.
2. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
3. In **Computer Name**, type **INET1**.
4. Click **OK**.
5. When you are prompted that you must restart the computer, click **OK**.
6. On the **System Properties** dialog box, click **Close**.
7. When you are prompted to restart the computer, click **Restart Now**.
9. After the computer has restarted, log on with the local Administrator account.
10. In **Initial Configuration Tasks**, click **Do not show this window at logon**, and then click **Close**.

Install the Web Server (IIS) and DNS server roles

Next, install role services for INET1, which will act as an Internet Web and DNS server for computers that are connected to the Internet subnet.

To install the IIS and DNS server roles

1. In Server Manager, under **Roles Summary**, click **Add Roles**, and then click **Next**.
2. On the **Select Server Roles** page, select the **Web Server (IIS)** and **DNS Server** check boxes, and then click **Next**.
3. Click **Next** twice to accept the default Web server settings, and then click **Install**.
4. Verify that all installations were successful, and then click **Close**.

Create DNS A records

Next, create DNS A records for INET1's and DA1's IPv4 addresses on the Internet subnet and for the name `crl.contoso.com`.

To create A records

1. Click **Start**, point to **Administrative Tools**, and then click **DNS**.
2. In the console tree of DNS Manager, open **INET1**.
3. Right-click **Forward Lookup Zones**, click **New Zone**, and then click **Next**.
4. On the **Zone Type** page, click **Next**.
5. On the **Zone Name** page, type `isp.example.com`, and then click **Next**.
6. On the **Dynamic Update** page, click **Next**, and then click **Finish**.
7. In the console tree, right click `isp.example.com`, and then click **New Host (A or AAAA)**.
8. In **Name**, type **INET1**. In **IP address**, type `131.107.0.1`. Click **Add Host**.
9. Click **OK**, and then click **Done**.
10. In the console tree, right-click **Forward Lookup Zones**, click **New Zone**, and then click **Next**.
11. On the **Zone Type** page, click **Next**.
12. On the **Zone Name** page, type `contoso.com`, and then click **Next**.
13. On the **Dynamic Update** page, click **Next**, and then click **Finish**.
14. In the console tree, right click `contoso.com`, and then click **New Host (A or AAAA)**.
15. In **Name**, type **da1**. In **IP address**, type `131.107.0.2`.
16. Click **Add Host**. Click **OK**.
17. In **Name**, type **crl**. In **IP address**, type `131.107.0.2`.
18. Click **Add Host**. Click **OK**, and then click **Done**.
19. Close the DNS console.

Install and configure DHCP

Next, configure INET1 as a DHCP server so that CLIENT1 can automatically configure itself when connecting to the Internet subnet.

▶ To install and configure the DHCP server role on INET1

1. Click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. Under **Roles Summary**, click **Add roles**, and then click **Next**.
3. On the **Select Server Roles** page, select the **DHCP Server** check box, and then click **Next** twice.
4. On the **Select Network Connection Bindings** page, verify that **131.107.0.1** is selected, and then click **Next**.
5. On the **Specify IPv4 DNS Server Settings** page, type **isp.example.com** in **Parent domain**.
6. Type **131.107.0.1** under **Preferred DNS server IP address**, and click **Validate**. Verify that the result returned is **Valid**, and then click **Next**.
7. On the **Specify WINS Server Settings** page, accept the default setting of **WINS is not required on this network**, and then click **Next**.
8. On the **Add or Edit DHCP Scopes** page, click **Add**.
9. In the **Add Scope** dialog box, type **Internet** next to **Scope Name**. Next to **Starting IP Address**, type **131.107.0.100**, next to **Ending IP Address**, type **131.107.0.150**, and next to **Subnet Mask**, type **255.255.255.0**.
10. Select the **Activate this scope** check box, click **OK**, and then click **Next**.
11. On the **Configure DHCPv6 Stateless Mode** page, select **Disable DHCPv6 stateless mode for this server**, and then click **Next**.
12. On the **Confirm Installation Selections** page, click **Install**.
13. Verify that the installation was successful, and then click **Close**.

Configure NAT1

NAT1 will run Windows 7, and it will act as a NAT between the Internet and Homenet subnets. NAT1 configuration consists of the following steps:

- Install the operating system.
- Configure Network Connections properties.
- Configure Internet Connection Sharing.

Note

NAT1 must have two network adapters installed.

Install the operating system on NAT1

▶ **To install Windows 7 on NAT1**

1. Connect one network adapter to the Internet subnet and the other network adapter to the Homenet subnet.
2. Start the installation of Windows 7.
3. When you are prompted for a user name, type **User1**. When you are prompted for a computer name, type **NAT1**.
4. When you are prompted for a password, type a strong password twice.
5. When you are prompted for protection settings, click **Use recommended settings**.
6. When you are prompted for your computer's current location, click **Public**.

Configure Network Connections properties

Next, configure the names of the adapters in the Network Connections folder for the subnets to which they are connected.

▶ **To configure Network Connections properties**

1. Click **Start**, and then click **Control Panel**.
2. Under **Network and Internet**, click **View status and tasks**, and then click **Change adapter settings**.
3. In the **Network Connections** window, right-click the network connection that is connected to the Homenet subnet, and then click **Rename**.
4. Type **Homenet**, and then press ENTER.
5. In the **Network Connections** window, right-click the network connection that is

connected to the Internet subnet, and then click **Rename**.

6. Type **Internet**, and then press ENTER.
7. Leave the **Network Connections** window open for the next procedure.
8. Click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
9. To check network communication between NAT1 and INET1, in the Command Prompt window, type **ping inet1.isp.example.com**, and then press ENTER.
10. Verify that there are four responses from 131.107.0.1.
11. In the Command Prompt window, type **netsh interface 6to4 set state state=disabled**, and then press ENTER.
12. Close the Command Prompt window.

Configure Internet Connection Sharing

▶ To configure Internet Connection Sharing on NAT1

1. In the **Network Connections** window, right-click **Internet**, and then click **Properties**.
2. Click the **Sharing** tab, select **Allow other network users to connect through this computer's Internet connection**, and then click **OK**.

Configure CLIENT1

CLIENT1 is a computer that is running Windows 7 that you will use to demonstrate how DirectAccess works for remote computers. CLIENT1 configuration consists of the following steps:

- Install the operating system.
- Join CLIENT1 to the CORP domain.
- Add CLIENT1 to the DA_Clients security group.
- Verify the computer certificate on CLIENT1.
- Test access to intranet resources.
- Test access to the network location server.

- Test access to intranet resources from the Internet.

Install the operating system on CLIENT1

▶ To install the operating system on CLIENT1

1. Connect CLIENT1 to the Corpnet subnet.
2. Start the installation of Windows 7 Enterprise or Ultimate.
3. When you are prompted for a user name, type **User1**. When you are prompted for a computer name, type **CLIENT1**.
4. When you are prompted for a password, type a strong password twice.
5. When you are prompted for protection settings, click **Use recommended settings**.
6. When you are prompted for your computer's current location, click **Work**.

User Account Control

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

Join CLIENT1 to the CORP domain

▶ To join CLIENT1 to the CORP domain

1. Click **Start**, right-click **Computer**, and then click **Properties**.
2. Under **Computer name, domain, and workgroup settings**, click **Change settings**.
3. In the **System Properties** dialog box, click **Change**.
4. In the **Computer Name/Domain Changes** dialog box, click **Domain**, type **corp.contoso.com**, and then click **OK**.
5. When you are prompted for a user name and password, type the user name and password for the User1 domain account, and then click **OK**.
6. When you see a dialog box that welcomes you to the corp.contoso.com domain, click **OK**.

7. When you see a dialog box that prompts you to restart the computer, click **OK**.
8. In the **System Properties** dialog box, click **Close**.
9. In the dialog box that prompts you to restart the computer, do not click anything and proceed to the following procedure.

Add CLIENT1 to the DA_Clients security group

Next, add CLIENT1 to the DA_Clients security group so that it can receive DirectAccess client settings through Group Policy.

To add CLIENT1 to the DirectAccess client computers security group

1. On DC1, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, open **corp.contoso.com**, and then **Users**.
3. In the details pane, double-click **DA_Clients**.
4. In the **DA_Clients Properties** dialog box, click the **Members** tab, and then click **Add**.
5. In the **Select Users, Contacts, Computers, or Groups** dialog box, click **Object Types**, click **Computers**, and then click **OK**.
6. Under **Enter the object names to select (examples)**, type **CLIENT1**, and then click **OK**.
7. Verify that **CLIENT1** is displayed below **Members**, and then click **OK**.
8. Close the Active Directory Users and Computers console.
9. On CLIENT1, in the dialog box that prompts you to restart the computer, click **Restart Now**.
10. After CLIENT1 restarts, click **Switch User**, click **Other User**, and then log on to the CORP domain with the User1 account.

Verify the computer certificate on CLIENT1

Next, verify that a computer certificate has been installed on CLIENT1.

To verify that CLIENT1 has a computer certificate installed

1. On CLIENT1, click **Start**, type **mmc**, and then press ENTER.

2. Click **File**, and then click **Add/Remove Snap-in**.
3. Click **Certificates**, click **Add**, select **Computer account**, click **Next**, select **Local computer**, click **Finish**, and then click **OK**.
4. In the console tree, open **Certificates (Local Computer)\Personal\Certificates**.
5. In the details pane, verify that a certificate was enrolled with **Intended Purposes** of **Client Authentication** and **Server Authentication**. This certificate will be used for authentication with DA1.
6. Close the console window. When you are prompted to save settings, click **No**.

Test access to intranet resources

Next, verify that intranet Web and file share resources on APP1 can be accessed by CLIENT1.

To test access to intranet resources from CLIENT1

1. From the taskbar, click the Internet Explorer® icon.
2. In the **Welcome to Internet Explorer 8** window, click **Next**. In the **Turn on Suggested Sites** window, click **No, don't turn on**, and then click **Next**. In the **Choose your settings** dialog box, click **Use express settings**, and then click **Finish**.
3. In the Toolbar, click **Tools**, and then click **Internet Options**. For **Home page**, click **Use blank**, and then click **OK**.
4. In the Address bar, type **http://app1.corp.contoso.com/**, and then press ENTER. You should see the default IIS 7 Web page for APP1.
5. Leave the Internet Explorer window open.
6. Click **Start**, type **\\app1\Files**, and then press ENTER.
7. You should see a folder window with the contents of the Files shared folder.
8. In the **Files** shared folder window, double-click the **Example.txt** file. You should see the contents of the Example.txt file.
9. Close the **example.txt - Notepad** and the **Files** shared folder windows.

Test access to the network location server

Next, verify that the intranet network location server can be accessed by CLIENT1.

▶ **To test access to the network location server from CLIENT1**

1. From the taskbar, click the Internet Explorer icon.
2. In the Address bar, type **https://nls.corp.contoso.com**, and then press ENTER. You should see the default IIS 7 Web page.
3. Close Internet Explorer.

Test access to intranet resources from the Internet subnet

Next, connect CLIENT1 to the Internet subnet and demonstrate that the Web and file share resources on APP1 are not accessible from the Internet.

▶ **To test access to intranet resources from CLIENT1 when connected to the Internet subnet**

1. Unplug the Ethernet cable of CLIENT1 from the switch for the Corpnet subnet and plug it into the switch for the Internet subnet.
2. From the taskbar, click the Internet Explorer icon.
3. In the **Address** bar, type **http://app1.corp.contoso.com/**, and then press ENTER. You should see the **Internet Explorer cannot display the webpage** message.
4. Close the Internet Explorer window.
5. Click **Start**, type **\\app1\Files**, and then press ENTER.
6. You should see the **Windows cannot access \\app1\files** message. Click **Cancel**.
7. Unplug the Ethernet cable of CLIENT1 from the switch for the Internet subnet and plug it into the switch for the Corpnet subnet.

Configuring DirectAccess

Use the following procedures to configure DirectAccess and verify the resulting intranet configuration:

- Install the DirectAccess feature on DA1.
- Run the DirectAccess Setup Wizard on DA1.
- Update IPv6 settings on APP1 and DC1.

- Update Group Policy and IPv6 settings on CLIENT1.
- Verify ISATAP-based connectivity.

Install the DirectAccess feature on DA1

Before you can run the DirectAccess Setup Wizard, you must install the DirectAccess feature on DA1.

▶ To install the DirectAccess feature from Server Manager

1. If needed, log on to DA1 with the User1 user account and password.
2. If needed, click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
3. In the main window, under **Features Summary**, click **Add features**
4. On the **Select Features** page, select **DirectAccess Management Console**.
5. In the **Add Features Wizard** window, click **Add Required Features**.
6. On the **Select Features** page, click **Next**.
7. On the **Confirm Installation Selections** page, click **Install**.
8. On the **Installation Results** page, click **Close**.

Run the DirectAccess Setup wizard on DA1

Next, run the DirectAccess Setup Wizard to configure DA1 and the Group Policy settings for DirectAccess clients.

▶ To run the DirectAccess Setup Wizard

1. Click **Start**, point to **Administrative Tools**, and then click **DirectAccess Management**.
2. In the console tree, click **Setup**. In the details pane, click **Configure** for step 1.
3. On the **DirectAccess Client Setup** page, click **Add**.
4. In the **Select Group** dialog box, type **DA_Clients**, click **OK**, and then click **Finish**.
5. Click **Configure** for step 2.
6. On the **Connectivity** page, for **Interface connected to the Internet**, select **Internet**. For **Interface connected to the internal network**, select **Corpnet**. Click **Next**.

7. On the **Certificate Components** page, for **Select the root certificate to which remote client certificates must chain**, click **Browse**. In the list of certificates, click the corp-DC1-CA root certificate, and then click **OK**.
8. For **Select the certificate that will be used to secure remote client connectivity over HTTPS**, click **Browse**. In the list of certificates, click the certificate named **IP-HTTPS Certificate**, and then click **OK**. Click **Finish**.
9. Click **Configure** for step 3.
10. On the **Location** page, click **Network Location server is run on a highly available server**, type **https://nls.corp.contoso.com**, click **Validate**, and then click **Next**.
11. On the **DNS and Domain Controller** page, note the entry for the name **corp.contoso.com** with the IPv6 address **2002:836b:2:1:0:5efe:10.0.0.1**. This IPv6 address is assigned to DC1 and is composed of a 6to4 network prefix (2002:836b:2:1::/64) and an ISATAP-based interface identifier (::0:5efe:10.0.0.1). Click **Next**.
12. On the **Management** page, click **Finish**.
13. Click **Configure** for step 4. On the DirectAccess Application Server Setup page, click **Finish**.
14. Click **Save**, and then click **Finish**.
15. In the **DirectAccess Review** dialog box, click **Apply**. In the **DirectAccess Policy Configuration** message box, click **OK**.

Update IPv6 settings on APP1

Next, force APP1 to refresh its IPv6 settings so that it can immediately configure itself as an ISATAP host.

To update IPv6 settings on APP1

1. On APP1, click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
2. From the Command Prompt window, type **net stop iphlpsvc**, press ENTER, type **net start iphlpsvc**, and then press ENTER.
3. Close the Command Prompt window.

Update IPv6 settings on DC1

Next, force DC1 to refresh its IPv6 settings so that it can immediately configure itself as an ISATAP host.

▶ To update IPv6 settings on DC1

1. On DC1, click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
2. From the Command Prompt window, type **net stop iphlpsvc**, press ENTER, type **net start iphlpsvc**, and then press ENTER.
3. Close the Command Prompt window.

Update Group Policy and IPv6 settings on CLIENT1

Next, force CLIENT1 to update its Group Policy settings so that it is configured as a DirectAccess client, and then immediately update its IPv6 settings so that it can configure itself as an ISATAP host.

▶ To update Group Policy and IPv6 settings on CLIENT1

1. On CLIENT1, click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
2. From the Command Prompt window, type **gpupdate**, and then press ENTER.
3. From the Command Prompt window, type **net stop iphlpsvc**, press ENTER, type **net start iphlpsvc**, and then press ENTER.
4. Leave the Command Prompt window open for the next procedure.

Verify ISATAP-based connectivity

Next, verify that CLIENT1 can connect to DC1 and APP1 by using IPv6 and ISATAP-based addresses.

▶ To verify ISATAP-based connectivity to DC1 and APP1

1. On CLIENT1, from the Command Prompt window, type **ipconfig /flushdns**, and then press ENTER.
2. From the Command Prompt window, type **ping 2002:836b:2:1::5efe:10.0.0.1**, and then press ENTER. This is the ISATAP-based address of DC1. You should see four successful

replies.

3. From the Command Prompt window, type **ping 2002:836b:2:1::5efe:10.0.0.3**, and then press ENTER. This is the ISATAP-based address of APP1. You should see four successful replies.
4. From the Command Prompt window, type **ping dc1.corp.contoso.com**, and then press ENTER. You should see the name dc1.corp.contoso.com resolved to the IPv6 address 2002:836b:2:1::5efe:10.0.0.1 and four successful replies.
5. From the Command Prompt window, type **ping app1.corp.contoso.com**, and then press ENTER. You should see the name app1.corp.contoso.com resolved to the IPv6 address 2002:836b:2:1::5efe:10.0.0.3 and four successful replies.
6. Leave the Command Prompt window open for the next procedure.

Verifying DirectAccess functionality for CLIENT1 when connected to the Internet subnet

The following procedures verify DirectAccess functionality for CLIENT1 when it is connected to the Internet subnet:

- Connect CLIENT1 to the Internet subnet.
- Verify connectivity to Internet resources.
- Verify intranet access to Web and shared folder resources on APP1.
- Examine the CLIENT1 IPv6 configuration.

Connect CLIENT1 to the Internet subnet

This procedure simulates the roaming of CLIENT1 from an intranet (the Corpnet subnet) to the Internet (the Internet subnet).

To connect CLIENT1 to the Internet subnet

1. Unplug the Ethernet cable of CLIENT1 from the switch for the Corpnet subnet and then plug it into the switch for the Internet subnet. Wait until the network icon in the notification area of the desktop displays a yellow caution sign.
2. To verify that the proper IPv4 address has been configured, from the Command Prompt window, type **ipconfig**, and then press ENTER.

3. In the display of the Ipconfig.exe tool, verify that the interface named Local Area Connection has an IPv4 address that begins with **131.107**.
4. Leave the Command Prompt window open for the next procedure.

Verify connectivity to Internet resources

Next, verify that CLIENT1 can use Internet DNS servers and access Internet resources.

▶ To verify connectivity to Internet resources

1. From the Command Prompt window, type **ping inet1.isp.example.com**, and then press ENTER.
2. You should see the name **inet1.isp.example.com** resolved to the IPv4 address **131.107.0.1** and four successful replies.
3. From the taskbar, click the Internet Explorer icon.
4. In the Address bar, type **http://inet1.isp.example.com/**, and then press ENTER. You should see the default IIS 7 Web page for INET1.
5. Leave the Internet Explorer window open for the next procedure.

Verify intranet access to Web and shared folder resources on APP1

Next, verify that CLIENT1 can access intranet resources as if it was connected to the Corpnetsubnet.

▶ To verify that CLIENT1 can access intranet resources

1. From the Command Prompt window, type **ping app1**, and then press ENTER.
2. You should see the name **app1.corp.contoso.com** resolved to the IPv6 address **2002:836b:2:1:0:5efe:10.0.0.3** and four successful replies.
3. In Internet Explorer, in the Address bar, type **http://app1.corp.contoso.com/**, press ENTER, and then press **F5**. You should see the default IIS 7 Web page for APP1.
4. Close Internet Explorer.
5. Click **Start**, type **\\app1\files**, and then press ENTER. You should see a folder window with the contents of the **Files** shared folder.
6. In the **Files** shared folder window, double-click the **Example.txt** file.

7. Close the **example.txt - Notepad** window and the **Files** shared folder window.

**Note**

If you encounter problems with these steps, see the [General Methodology for Troubleshooting DirectAccess Connections](#) topic in the [DirectAccess Troubleshooting Guide](#).

Examine the CLIENT1 IPv6 configuration

Next, examine the IPv6 configuration of CLIENT1.

To examine CLIENT1's IPv6 configuration

1. From the Command Prompt window, type **ipconfig**, and then press ENTER.
2. From the display of the Ipconfig.exe tool, notice that an interface named **Tunnel adapter 6TO4 Adapter** has an IPv6 address that begins with **2002:836b:**. This is a 6to4 address based on an IPv4 address that begins with 131.107. Notice that this tunnel interface has a default gateway of 2002:836b:2::836b:2, which corresponds to the 6to4 address of DA1 (131.107.0.2 in colon-hexadecimal notation is 836b:2). CLIENT1 uses 6to4 and this default gateway to tunnel IPv6 traffic to DA1.

Verifying DirectAccess functionality for CLIENT1 when connected to the Homenet subnet

The following procedures verify DirectAccess functionality for CLIENT1 when it is connected to the Homenet subnet:

- Connect CLIENT1 to the Homenet subnet.
- Verify connectivity to Internet resources.
- Verify intranet access to Web and shared folder resources on APP1.
- Examine the CLIENT1 IPv6 configuration.
- Disable Teredo connectivity on CLIENT1.
- Verify intranet access to Web and shared folder resources on APP1.
- Enable Teredo connectivity on CLIENT1.
- Connect CLIENT1 to the Corpnet subnet.

Connect CLIENT1 to the Homenet subnet

This procedure simulates the roaming of CLIENT1 from the Internet (the Internet subnet) to a home network that is connected to the Internet (the Homenet subnet).

▶ To connect CLIENT1 to the Homenet subnet

1. Unplug the Ethernet cable of CLIENT1 from the switch for the Internet subnet and then plug it into the switch for the Homenet subnet. Wait until the network icon in the notification area of the desktop displays a yellow caution sign.
2. To verify that the proper IPv4 address has been configured, from the Command Prompt window, type **ipconfig**, and then press ENTER.
3. In the display of the Ipconfig.exe tool, verify that the interface named Local Area Connection has an IPv4 address starting with **192.168.137**.
4. Leave the Command Prompt window open for the next procedure.

Verify connectivity to Internet resources

Next, verify that CLIENT1 can use Internet DNS servers and access Internet resources.

▶ To verify connectivity to Internet resources

1. From the Command Prompt window, type **ping inet1.isp.example.com**, and then press ENTER.
2. You should see the name **inet1.isp.example.com** resolved to the IPv4 address **131.107.0.1** and four successful replies.
3. In the task bar, click the Internet Explorer icon.
4. In the Address bar, type **http://inet1.isp.example.com/**, press ENTER, and then press **F5**. You should see the default IIS 7 Web page for INET1.
5. Leave the Internet Explorer window open for the next procedure.

Verify intranet access to Web and shared folder resources on APP1

Next, verify that CLIENT1 can access intranet resources as if it was connected to the Corpnet subnet.

▶ To verify that CLIENT1 can access intranet resources

1. In the Address bar of Internet Explorer, type **http://app1.corp.contoso.com/**, and then

press ENTER. You should see the default IIS 7 Web page for APP1.

2. Close Internet Explorer.
3. Click **Start**, type `\\app1\files`, and then press ENTER.
4. You should see a folder window with the contents of the Files shared folder.
5. In the **Files** shared folder window, double-click the **Example.txt** file.
6. Close the **example.txt - Notepad** window and the **Files** shared folder window.

Examine the CLIENT1 IPv6 configuration

Next, examine the IPv6 configuration of CLIENT1.

To examine the CLIENT1 IPv6 configuration

1. From the Command Prompt window, type **ipconfig**, and then press ENTER.
2. From the display of the Ipconfig.exe tool, notice that an interface has an IPv6 address that starts with **2001:**. This is a Teredo address assigned by DA1. When CLIENT1 is behind a NAT that does not support 6to4 router functionality, CLIENT1 uses Teredo to tunnel IPv6 traffic to DA1.
3. Leave the Command Prompt window open for the next procedure.

Disable Teredo connectivity on CLIENT1

This procedure simulates the roaming of CLIENT1 from a home network to a private network with a Web proxy or firewall that does not forward Teredo traffic. In this environment, CLIENT1 uses the IP-HTTPS protocol to connect to the DirectAccess server.

To disable Teredo connectivity on CLIENT1

1. From the Command Prompt window, type **netsh interface teredo set state disabled**, and then press ENTER.
2. Unplug the Ethernet cable of CLIENT1 from the switch for the Homenet subnet and then plug it back into the switch for the Homenet subnet. Wait until the network icon in the notification area of the desktop displays a yellow caution sign.
3. From the Command Prompt window, type **ipconfig**, and then press ENTER.
4. In the display of the Ipconfig.exe tool, verify that there is an interface named

IPHTTPS interface with an IPv6 address that starts with **2002:836b:2:2**. This is an address assigned to the IP-HTTPS interface by DA1. When CLIENT1 is behind a Web proxy or firewall that does not forward Teredo traffic, CLIENT1 uses IP-HTTPS to tunnel IPv6 traffic to DA1.

5. Leave the Command Prompt window open for the next procedure.

Verify intranet access to Web and file share resources on APP1

Next, verify that CLIENT1 can access intranet resources as if it was connected to the Corpnet subnet.

To verify that CLIENT1 can access intranet resources

1. In the Address bar, type **http://app1.corp.contoso.com/**, press ENTER, and then press **F5**. You should see the default IIS 7 Web page for APP1.
2. Close Internet Explorer.
3. Click **Start**, type **\\app1\files**, and then press ENTER.
4. You should see a folder window with the contents of the Files shared folder.
5. In the **Files** shared folder window, double-click the **Example.txt** file.
6. Close the **example.txt - Notepad** window and the **Files** shared folder window.

Enable Teredo connectivity on CLIENT1

In this procedure, you enable Teredo connectivity on CLIENT1.

To enable Teredo connectivity on CLIENT1

1. From the Command Prompt window, type **netsh interface teredo set state enterpriseclient**, and then press ENTER.
2. From the Command Prompt window, type **ipconfig**, and then press ENTER.
3. In the display of the Ipconfig.exe tool, verify that an interface has an IPv6 address that starts with **2001:**.

Connect CLIENT1 to the Corpnet subnet

Next, connect CLIENT1 to the Corpnet subnet to test intranet connectivity for the last time.

▶ **To connect CLIENT1 to the Corpnet subnet**

1. Unplug the Ethernet cable of CLIENT1 from the switch for the Homenet subnet and plug it into the switch for the Corpnet subnet.
2. Log on to CLIENT1 by using the User1 account.
3. In the taskbar, click the Internet Explorer icon.
4. In the Address bar of Internet Explorer, type **http://app1.corp.contoso.com/**, press ENTER, and then press **F5**. You should see the default IIS 7 Web page for APP1.
5. Close Internet Explorer.
6. Click Start, type **\\app1\files**, and then press ENTER.
7. You should see a folder window with the contents of the Files shared folder.
8. In the **Files** shared folder window, double-click the **Example.txt** file.
9. Close the **example.txt - Notepad** window and the **Files** shared folder window.

Additional Resources

To learn DirectAccess troubleshooting tools and techniques using the DirectAccess test lab described in this document, see the [Step by Step Guide: Troubleshoot DirectAccess in a Test Lab](#).

For the design and configuration of your pilot or production deployment of DirectAccess, see the [DirectAccess Design Guide](#) and the [DirectAccess Deployment Guide](#).

For information about troubleshooting DirectAccess, see the [DirectAccess Troubleshooting Guide](#).

For more information about DirectAccess, see the [DirectAccess Getting Started Web page](#) and the [DirectAccess TechNet Web page](#).

Appendix

This appendix describes how to change the default User Account Control (UAC) behavior in Windows Server 2008 R2 and Windows 7.

Set UAC behavior of the elevation prompt for administrators

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

To set UAC behavior of the elevation prompt for administrators

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