



Introduction to DirectAccess in Windows Server 2012

Windows Server
2012



Hands-on lab

In this lab, you will configure a Windows 8 workgroup client to access the corporate network using DirectAccess technology, even though the client computer has never been in contact with the corporate network. You will configure DirectAccess on a server in the corporate network, configure Active Directory and create a computer account for the client computer, import a configuration file into the client computer, and then successfully have the client use DirectAccess to access the corporate network using IPv4.

Produced by HynesITe, Inc
Version 3.0
[2/18/2013-2/18/2013](#)



This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release. 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 companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. 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.

Copyright 2013 © Microsoft Corporation. All rights reserved.

Microsoft, Hyper-V, Internet Explorer, Windows, Windows PowerShell, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Introduction

Estimated time to complete this lab

30 minutes

Objectives

After completing this lab, you will be able to:

- Configure DirectAccess in Windows Server 2012.
- Configure a Windows 8 client to use DirectAccess to access the corporate network.

Prerequisites

Before working on this lab, you must have:

- Knowledge of networking components and Active Directory.

Overview of the lab

In this lab, you will configure a Windows 8 workgroup client to access the corporate network using DirectAccess technology, even though the client computer has never been in contact with the corporate network. You will configure DirectAccess on a server in the corporate network, configure Active Directory and create a computer account for the client computer, import a configuration file into the client computer, and then successfully have the client use DirectAccess to access the corporate network using IPv4.

Intended audience

This lab is intended for administrators who wish to use Windows Server 2012 to provide remote access to Windows 8 clients.

Virtual machine technology

This lab is completed using virtual machines that run on Windows Server 2012 Hyper-V technology. To log on to the virtual machines, press CTRL+ALT+END and enter your logon credentials.

Computers in this lab

This lab uses computers as described in the following table. Before you begin the lab, you must ensure that the virtual machines are started and then log on to the computers.

Virtual Machine	Role
DC	Domain controller for contoso.com
DAServer	DirectAccess server connecting Contoso to the Internet
WLANRouter	Router connecting the Internet and the client network
DAClient	Windows 8 client in a workgroup

⚠ All user accounts in this lab use the password **Passw0rd!**

Note regarding pre-release software

Introduction to DirectAccess in Windows Server 2012

Portions of this lab include software that is not yet released, and as such may still contain active or known issues. While every effort has been made to ensure this lab functions as written, unknown or unanticipated results may be encountered as a result of using pre-release software.

Note regarding user account control

Some steps in this lab may be subject to user account control. User account control is a technology which provides additional security to computers by requesting that users confirm actions that require administrative rights. Tasks that generate a user account control confirmation are denoted using a shield icon. If you encounter a shield icon, confirm your action by selecting the appropriate button in the dialog box that is presented.

Exercise 1: Create a Security Group for DirectAccess Clients

When DirectAccess is configured, it automatically creates Group Policy objects (GPO) containing DirectAccess settings to configure to DirectAccess clients and servers. By default, the DirectAccess Getting Started Wizard applies the client GPO to mobile computers in the Domain Computers security global group. The procedures in this lab do not use the default setting, but instead create a new security group to filter the GPO to apply only to specific DirectAccess clients.

Create a security group for DirectAccess client computers

In this step, you will create a security group for Direct Access clients.

✎ Log on to **DC** as **Contoso\Administrator** using a password of **Passw0rd!**

1. On **DC**, on the Start screen, click **Active Directory Administrative Center**.
 - ✎ NOTE: The Start screen may not appear when you log on initially. To invoke the Start screen, hover the mouse pointer in the upper right corner of the screen, and then click Start. Alternatively, you can hover the mouse pointer in the lower left corner of the screen, and then click when the thumbnail of the Start screen appears.
2. In the console tree, expand **contoso.com**, and then double-click **Users**.
3. In the **Tasks** pane, click **New**, and then click **Group**.
4. In the Create Group dialog box, in the Group name, type **DA_Clients**.
5. Click **OK** to close the Create Group dialog box.
6. Close the Active Directory Administrative Center console.

✎ NOTE: The above steps can also be completed using the following Windows PowerShell command.

```
↩ New-ADGroup -GroupScope global -Name DA_Clients
```

Exercise 2: Install the Remote Access Server Role

The Remote Access server role in Windows Server 2012 combines the DirectAccess feature and the Routing and Remote Access 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.

Install the Remote Access server role

In this step, you will install the Remote Access server role.

✎ Log on to **DAServer** as **Contoso\Administrator** using a password of **Passw0rd!**

1. Open **Server Manager**.
2. In the Server Manager Dashboard console, under Configure this local server, click **Add roles and features**.
3. Click **Next** three times.
4. On the Select Server Roles page, select **Remote Access**, click **Add Features** when prompted, and then click **Next**.
5. Click **Next** five times to accept the defaults for features, remote access role services, and web server role services.
6. On the Confirm installation selections page, click **Install**.

6. ⚠ **NOTE:** [This installation can take up to 5 minutes to complete. This is expected.](#)

7. Wait for the feature installations to complete, and then click **Close**.
✎ **NOTE:** Steps 1 through 7 can be completed using the following command.

```
↪ Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

Exercise 3: 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.

In this step, you will configure DirectAccess on the DirectAccess server.

✍ Ensure you are logged on to **DAServer** as **Contoso\Administrator** using a password of **Passw0rd!**

1. On the Start screen, click **Remote Access Management**.
 - ✦ To invoke the Start screen, you can hover the mouse pointer in the upper right corner of the screen, and then click Start. Alternatively, you can hover the mouse pointer in the lower left corner of the screen, and click when the thumbnail of the Start screen appears.
2. In the Remote Access Management console, click **Run the Getting Started Wizard**.
3. Click **Deploy both DirectAccess and VPN (recommended)**.
4. On the Remote Access Server Setup page, verify that **Edge** is selected as the network topology.
5. On the same page, type **206.10.15.1** as the IPv4 address that will be used by remote access clients to connect, and then click **Next**.
 - ✦ NOTE: In addition to an IP address, you can also use a Fully Qualified Domain Name (FQDN), such as `Daserver.contoso.com`.
 - ✦ NOTE: By default, the Getting Started Wizard deploys the DirectAccess settings to all mobile computers in the domain by applying a WMI filter to the client settings GPO. This may not be appropriate for some environments; therefore you will perform the following steps to change the client security group setting for DirectAccess from Domain Computers to DA_Clients.
6. On the Configure Remote Access page, click the **here** link to edit the wizard settings.
7. In the Remote Access Review dialog box, next to Remote Clients, click **Change**.
8. In the Select Groups window, clear the **Enable DirectAccess for mobile computers only** check box.
 - ✦ NOTE: This setting allows the GPO to use a WMI filter to detect mobile clients and filter the application of the GPO only to them.
9. Click **Domain Computers (Contoso\Domain Computers)**, and then click **Remove**.
10. Click **Add**, type **DA_Clients**, and then click **OK**.
11. Click **Next**.

Introduction to DirectAccess in Windows Server 2012

12. In the DirectAccess Client setup window, double-click the white box next to the arrow with the asterisk.
13. In the Type drop-down list, click **Ping**, and then in the text box, type **dc.contoso.com**.
14. Click **Validate**. A green check mark will appear indicating a successful ping.
15. Click **Add**.
16. In the DirectAccess Client setup window, note the friendly name, Workplace Connection, of the DirectAccess connection that will be created on clients.

Helpdesk email address:

DirectAccess connection name:

Allow DirectAccess clients to use local name resolution

17. In the DirectAccess Client setup window, click **Finish**.
18. On the Remote Access Review page, click **OK**, and then click **Finish**.
 - ✦ NOTE: As the wizard runs, you can click the More details arrow to reveal the actions being performed.
 - ✦ NOTE: The wizard will automatically provision self-signed certificates for IP-HTTPS and the Network Location Server. You can configure DirectAccess to use certificates issued by a Public Key Infrastructure (PKI) Certificate Authority. The wizard will also automatically enable Kerberos proxy and enable NAT64 and DNS64 for protocol translation in the IPv4-only environment.
 - ✦ NOTE: The wizard automatically creates two Group Policy objects (GPO) containing DirectAccess settings. One GPO is called DirectAccess Server Settings and is filtered to apply the settings only to the DirectAccess server computer account. The second GPO is called DirectAccess Client Settings and is filtered to apply settings to the DA_Clients global group previously created. Since the wizard detects that it is using Domain Admin credentials, it will also link both GPOs to the root of the domain. The GPOs can be created using Domain User credentials and later linked using Domain Admin credentials if necessary.
 - ✦ NOTE: The wizard will complete with a warning, because the name on the certificate provisioned is not suitable for NLB or multisite deployments.

19. After the wizard successfully completes applying the configuration, click **Close**.

19. —

until the status of all monitors display the message **Working**.

- ✦ NOTE: You may have to refresh the display to see the change in status. To do so, in the Tasks pane under Monitoring, click Refresh periodically to update the display.

21. [Close the Remote Access Management console](#)

Exercise 4: Prepare for the Client to Join the Domain

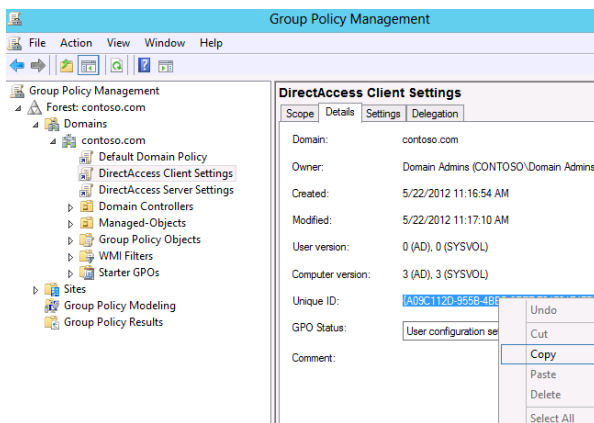
To have a workgroup client join the domain when not connected to the corporate network, a system administrator can create a file that contains all the required information and then provide that file to the client. The file contains the security information to join the domain as well as configuration information, such as registry settings to configure the client for DirectAccess. In this exercise, this file will be used by the client to configure itself to join the domain even though it is not in contact with the corporate network or a domain controller.

Create an offline domain join file for the client

In this step, you will create an offline domain join file for the client.

 If not already logged on, log on to DC as **Contoso\Administrator** using a password of **Passw0rd!**

1. Open a **Windows PowerShell** window. [You can use the shortcut in the task bar to open it.](#)
2. At the command prompt, type **GPMC.MSC** to open the Group Policy Management Console.
3. In the console tree, under Domains, expand the **contoso.com** domain.
4. In the console tree, click **Direct Access Client Settings**, and then click **OK**.
5. In the Details pane, click the **Details** tab.
6. Highlight the entire Unique ID string, including the braces, right-click the **Unique ID**, and then click **Copy**. Record the **Unique ID** for the GPO.

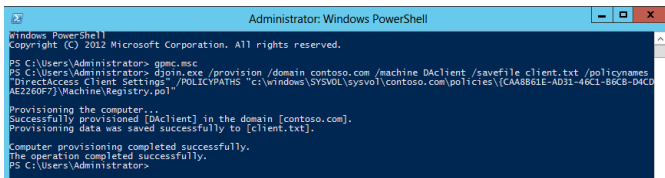


7. Minimize the GPMC console.
8. [At the Windows PowerShell command prompt](#), type the following command, pasting in the Unique ID in the string:

Introduction to DirectAccess in Windows Server 2012

```
↪ Djoin.exe /provision /domain contoso.com /machine DAclient /savefile client.txt /policynames "DirectAccess Client Settings" /POLICYPATHS "c:\windows\SYSTEM32\sysvol\contoso.com\policies\[unique ID of Group Policy Object copied in previous step]\Machine\Registry.pol"
```

- ★ NOTE: You can also use the tab complete method to enumerate the path to GPO, or you can open Windows Explorer, navigate to the folder containing the registry.pol file for the DirectAccess Client Settings GPO, copy the file path, and paste the file path into the command.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> gpic.msc
PS C:\Users\Administrator> djoin.exe /provision /domain contoso.com /machine DAclient /savefile client.txt /policynames "DirectAccess Client Settings" /POLICYPATHS "c:\windows\SYSTEM32\sysvol\contoso.com\policies\{CA48861E-AD31-46C1-86C8-D4C0AE2260F7}\Machine\Registry.pol"
Provisioning the computer...
Successfully provisioned [DAclient] in the domain [contoso.com].
Provisioning data was saved successfully to [client.txt].
Computer provisioning completed successfully.
The operation completed successfully.
PS C:\Users\Administrator>
```

9. At the Windows PowerShell command prompt, type the following command, and then press ENTER.

```
↪ Copy .\client.txt \\daserver\c$\inetpub\wwwroot\
```

- ★ NOTE: You are copying the client.txt file to the DAServer, which has IIS running and a web page accessible to the client via the Internet. This is done so the client can download the file and use the djoin.exe command to run the file to perform an offline domain join.

Add the client computer to the DA_Clients group

In this step, you will add the client computer to the DA_Clients group.

1. At the Windows PowerShell command prompt, type the following command, and then press ENTER.

```
↪ Add-ADGroupMember -Identity DA_Clients -Members DACLIENT$
```

- ★ NOTE: No output or confirmation is received. You can use ADAC to confirm that the CLIENT computer account was added to the DA_Clients group.

Prepare the file to be retrieved by the client

In this step, you will configure DAServer to host the client.txt file so the client can download it.

- ✍ If not already logged on to DAServer, log on to **DAServer** as **Contoso\Administrator** using a password of **Passw0rd!**

1. Open **Server Manager**.

Introduction to DirectAccess in Windows Server 2012

2. In the Console tree, click **IIS**.
3. In the Servers pane, right-click **DAServer**, and then click **Internet Information Services (IIS) Manager**.
4. In the Console tree, expand **DASERVER**, and then expand **Sites**.
✦ NOTE: If a dialog box appears, click No.

In the Console tree, expand **Sites** then click **Default Web Site**.

5. Right-click **Default Web Site**, and then click **Explore**.
6. Note that **client.txt** file is located in the folder.
⚠ **IMPORTANT:** Note the following security statement from Microsoft TechNet: The base64-encoded metadata blob that is created by the provisioning command contains very sensitive data. It should be treated just as securely as a plaintext password. The blob contains the machine account password and other information about the domain, including the domain name, the name of a domain controller, the security ID (SID) of the domain, and so on. If the blob is being transported physically or over the network, care must be taken to transport it securely.

Exercise 5: Configure the Client using the Offline Domain Join File

Configure the client using the offline domain join file

To have a workgroup client be able to join the domain, a system administrator can create a file that contains all the information required to join the domain. This file will be used on the client to configure itself to join the domain even though it is not in contact with a domain controller.

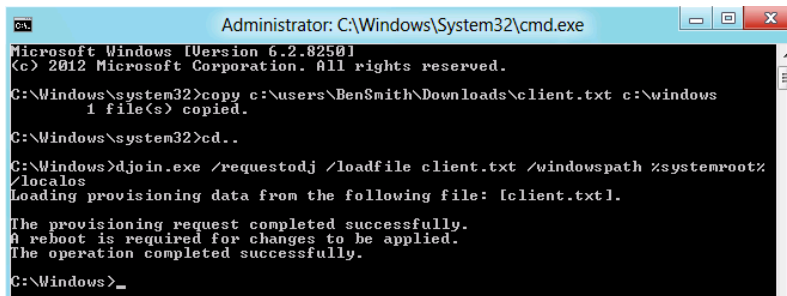
In this step, you will use the previously created offline domain join file to join the client computer to the domain.

✎ If not already logged on to DAClient, log on to **DAClient** as **BenSmith** using a password of **Passw0rd!**

1. Open the **Start Screen**.
2. Click **Internet Explorer**.
3. Navigate to **http://daserver.contoso.com/client.txt**.
4. Click **Save** to download the file.
5. When the download is complete, click **Close**.
6. Navigate to the **Start Screen**.
7. Type **CMD**
8. On the Start screen, right-click the **CMD** icon.
9. A check mark will appear next to the icon.
10. On the taskbar, click **Run as administrator**.
11. In the User Account Control prompt, click **Yes**.
12. At the command prompt, type the following commands, pressing ENTER after each one.

```
↵ copy c:\users\BenSmith\Downloads\client.txt c:\windows
↵ Cd..
↵ Djoin.exe /requestodj /loadfile client.txt /windowspath %systemroot%
  /localos
```

Introduction to DirectAccess in Windows Server 2012



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.2.8250]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>copy c:\users\BenSmith\Downloads\client.txt c:\windows
1 file(s) copied.

C:\Windows\system32>cd..

C:\Windows>djoin.exe /requestodj /loadfile client.txt /windowspath %systemroot%
/localos
Loading provisioning data from the following file: [client.txt].
The provisioning request completed successfully.
A reboot is required for changes to be applied.
The operation completed successfully.

C:\Windows>_
```

13. At the command prompt, type the following command, and then press ENTER to restart the client.

```
↩ Shutdown /t 0 /r /f
```

◆ [NOTE: The restart operation may take up to 5 minutes due to DA being established on boot. This is normal the first time you reboot after implementing DA, as Group Policy objects have to be applied.](#)

14. Wait one minute for the client to reboot.

Exercise 6: Test the Client using DirectAccess to Access the Corporate Network

When DirectAccess is configured on the client, it can join the domain and access resources as if it were directly connected to the corporate network.

Test the client computer using DirectAccess

In this step, you will test the DirectAccess client accessing the corporate network.

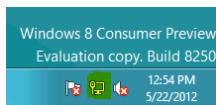
✎ Log on to **DAClient** as **BenSmith** using a password of **Passw0rd!**

1. On the Start screen, type **CMD**, and then click the **cmd** icon when it appears.
2. At the command prompt, type the following command, and then press ENTER.

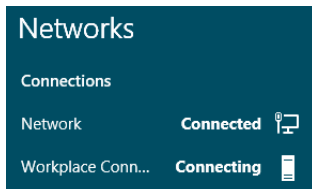
```
➔ Ping dc.contoso.com
```

✎ NOTE: The IPv6 address of the domain controller is returned.

3. In the System tray, click the **Network** icon.



4. In the Networks bar, note the **Workplace Connection** entry, which is the friendly name of the DirectAccess connection to the corporate network.



✎ NOTE: Notice that the status of the Workplace Connection entry is Connecting. If you were to hover your mouse over this Workplace Connection, you would see a message stating that network resources can't be reached. The reason for this is that you are not logged in as a domain user. However, a secure DirectAccess channel is open between the computer and the internal network. Unlike a typical VPN, DirectAccess is always on as long as the computer is outside the network and can communicate with the DirectAccess server over the Internet. DirectAccess enables "manage out" scenarios, whereby a remote computer can be remotely patched and updated, even if the user is not logged on.

5. At the command prompt, type the following command, and then press ENTER.

Introduction to DirectAccess in Windows Server 2012

↪ Powershell

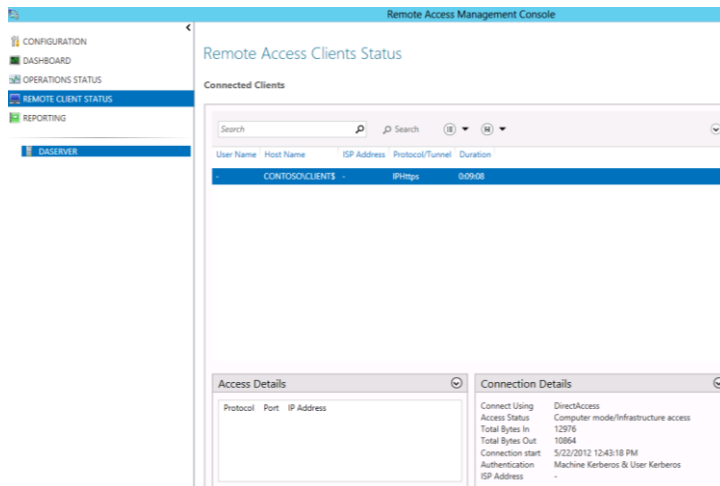
- At the Windows PowerShell command prompt, type the following command, and then press ENTER.

↪ Get-DAClientExperienceConfiguration

★ NOTE: Notice the DirectAccess client settings.

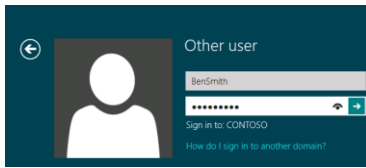
- Log on to **DAServer** as **Contoso\Administrator** using a password of **Passw0rd!**
- On the Start menu, click **Remote Access Management**.
- In the Console pane, click **Remote Client Status**.

★ NOTE: Notice that Client is connected via IPHttps. In the Connection Details pane in the bottom right of the screen, note the use of Kerberos for the Machine and the User. Also note that user name field is empty (recall that you are currently logged on to the DirectAccess client computer as a local user, not a domain user).



- Leave this console open for subsequent steps.
- Change from the DAServer to the **DAclient** computer.
- Log off the **DAclient** computer, clicking on your user name in the Start Menu and selecting **Sign Out**.
- On the **DAclient** computer, log on as **Contoso\BenSmith** using a password of **Passw0rd!**
 - ★ NOTE: You are logging on with the user's Contoso domain credentials.
 - ★⚠ WARNING: This first domain logon over DA may take up to 5 minutes to complete. This is expected. Subsequent logons will be much faster.

Introduction to DirectAccess in Windows Server 2012



14. On the Start screen, type **cmd**, and then click the **cmd** icon when it appears.
15. At the command prompt, type the following command, and then press ENTER.

```
↪ Gpresult /V | more
```

- ✦ NOTE: It may take a few minutes before policy information is available. If you still cannot see the policy information, you may need to log off, log back on, and then try again after a few minutes.
- ✦ NOTE: Notice that Group Policy from the Contoso domain is being applied to the client.

```
C:\Users\bensmith.CONTOSO>gpresult /U | more
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2012 Microsoft Corporation. All rights reserved.
Created on 5/22/2012 at 1:34:41 PM

-----
RSOP data for CONTOSO\bensmith on CLIENT : Logging Mode
-----
OS Configuration:      Member Workstation
OS Version:            6.2.8250
Site Name:             N/A
Roaming Profile:       N/A
Local Profile:         C:\Users\bensmith.CONTOSO
Connected over a slow link?: No

-----
USER SETTINGS
-----
CN=Ben Smith,OU=Users,OU=Managed-Objects,DC=contoso,DC=com
Last time Group Policy was applied: 5/22/2012 at 1:28:09 PM
Group Policy was applied from: DC.contoso.com
Group Policy slow link threshold: 500 Kbps
Domain Name:          CONTOSO
Domain Type:         Windows 2008 or later

-----
Applied Group Policy Objects
-----
N/A

-----
The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

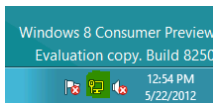
DirectAccess Server Settings
Filtering: Disabled (GPO)

Default Domain Policy
Filtering: Not Applied (Empty)

DirectAccess Client Settings
Filtering: Disabled (GPO)

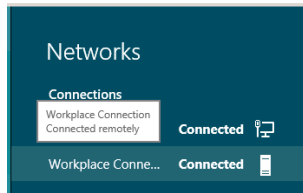
-----
The user is a part of the following security groups
-----
Domain Users
```

16. In the System tray, click the **Network** icon.



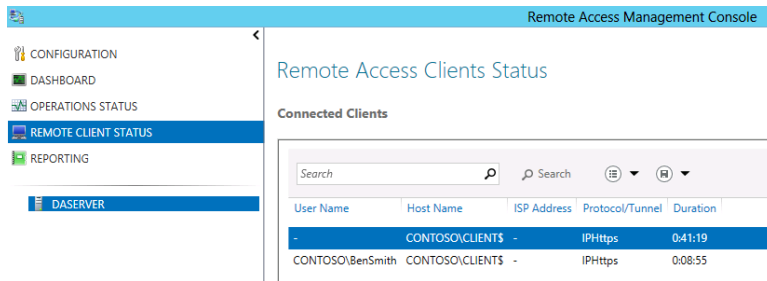
17. In the Networks bar, note the **Workplace Connection** entry now shows that the status is Connected.

Introduction to DirectAccess in Windows Server 2012



18. Switch to the **DAServer**.

19. In the Remote Access Management Console you left open in a previous step, [click refresh on the task pane](#), ~~note~~ **Note** **Contoso\BenSmith** now appears in the Connected Clients details pane.



This is the end of the lab.