WorkshopPLUS

Microsoft Azure Infrastructure as a Service (IaaS)

Configure a Point-to-Site VPN in the Portal (Classic)

Student Lab Manual

V1.9, September 5, 2015

Information in this document is subject to change without notice. The example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person 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, trademarked, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, MS, Windows, Windows NT, MSDN, Active Directory, BizTalk, SQL Server, SharePoint, Outlook, PowerPoint, FrontPage, Visual Basic, Visual C++, Visual J++, Visual InterDev, Visual SourceSafe, Visual C#, Visual J#,  and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names herein may be the trademarks of their respective owners.

Contents

[Configure a Point-to-Site VPN in the Portal 4](#_Toc429224598)

[Overview 4](#_Toc429224599)

[Objectives 5](#_Toc429224600)

[Configure the VPN client connection 5](#_Toc429224601)

[Prerequisites 5](#_Toc429224602)

[Exercises 5](#_Toc429224603)

[Exercise 1: Create a Point-to-Site VPN 5](#_Toc429224604)

[Task 1 - Create a Virtual Network 5](#_Toc429224605)

[Task 2 - Certificates 8](#_Toc429224606)

[Task 3 - Create the dynamic routing gateway 11](#_Toc429224607)

[Task 4 – Upload the root certificate 11](#_Toc429224608)

[Task 5 - Create the VPN Client configuration package 12](#_Toc429224609)

[Task 6 - Start the VPN Connection 12](#_Toc429224610)

[Task 7 - Verify the VPN Connection 13](#_Toc429224611)

[Summary 14](#_Toc429224612)

# Configure a Point-to-Site VPN in the Portal

## Overview

There are 3 main parts to configuring a point-to-site VPN. Each section of this lab will walk you through the tasks necessary, in order.

1. [Virtual networks and the virtual network gateway](http://localhost:57693/HOL.htm#bkmk_CreatingVNET) - First, you must configure the virtual network itself and the virtual network gateway. These steps can be accomplished by using the Management Portal.
2. [Certificates](http://localhost:57693/HOL.htm#bkmk_VPNCertificates) - Next, certificates must be generated and exported. The root certificate must then be uploaded to the Management Portal. The client certificate must be installed to each client computer that you want to connect to the VPN.
3. [VPN client configuration](http://localhost:57693/HOL.htm#bkmk_ClientConfig) - After the certificates are uploaded and installed, you can create, download, and install the client VPN configuration package. Once the package is installed, the VPN software on your client computer is configured to create a secure connection with your virtual network.

**NOTE:** In order to create a point-to-site VPN, you’ll need to first create a virtual network and a dynamic routing gateway. These procedures help you create the required virtual network configuration in the Management Portal. After completing this procedure, you’ll then create and distribute certificates to each client computer as well as configure the client computers with the proper VPN settings. For information and explanations about each setting available for virtual networks in the management portal wizard, see <http://msdn.microsoft.com/en-us/library/windowsazure/jj156074.aspx>.

## Objectives

In this hands-on lab, you will learn how to:

* Configure a new virtual network and virtual network gateway
* Create the certificates necessary to communicate with the P2S network

### Configure the VPN client connection

### Prerequisites

The following is required to complete this hands-on lab:

* A Microsoft Azure subscription [sign up for a free trial](http://aka.ms/WATK-FreeTrial)
* MakeCert.exe - if you already have Microsoft Visual Studio 2013 Professional or Ultimate edition, Makecert.exe should have been installed already.  Otherwise, you can find the tool in the .\Tools subfolder of the lab material (.\AzureIaaSWS\Tools)

**NOTE:** In order to run through the complete hands-on lab, you must have network connectivity.

## Exercises

This hands-on lab includes one exercise that walks through the process of creating a Point-to-Site VPN.

## Exercise 1: Create a Point-to-Site VPN

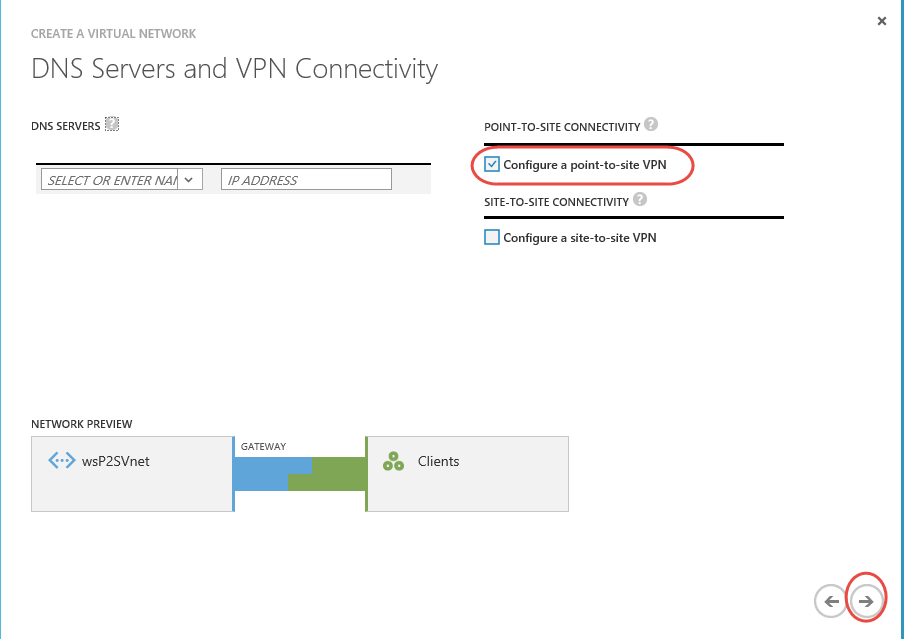
### ****Task 1 - Create a Virtual Network****

1. Log in to the **Microsoft Azure Management Portal at** <https://manage.windowsazure.com>.
2. In the lower left-hand corner of the screen, click **New**. In the navigation pane, click **Network Services | Virtual Networks | Custom Create**.
3. On the **Virtual Network Details** page, enter the following information, and then click the **Next** arrow on the lower right. For more information about the settings on the details page, see [Virtual Network Details page](http://msdn.microsoft.com/en-us/library/windowsazure/09926218-92ab-4f43-aa99-83ab4d355555#BKMK_VNetDetails).

* **Name**
* **Region** (data center location)

1. On the **DNS Servers and VPN Connectivity** page, enter the following information, and then click the **Next** arrow on the lower right.   
     
   NOTE: You can select both Point-To-Site and Site-To-Site configurations from this page. For the purposes of this topic, we will select to configure only Point-To-Site. For more information about the settings on this page, see [DNS Servers and VPN Connectivity page](http://msdn.microsoft.com/en-us/library/windowsazure/09926218-92ab-4f43-aa99-83ab4d355555#BKMK_VNETDNS).

* **DNS Servers** - you can leave this blank
* **Configure Point-To-Site VPN** (select checkbox)



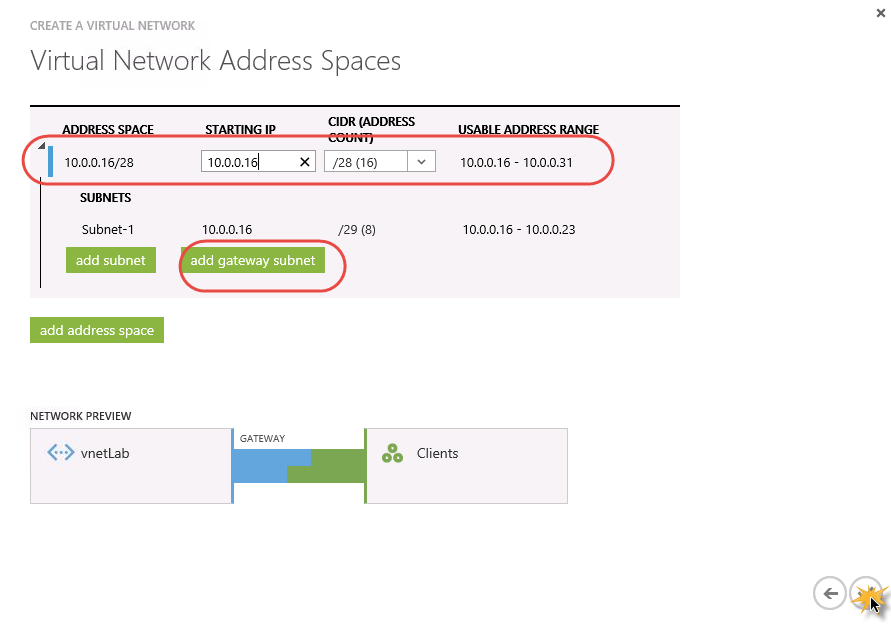
*Point-to-Site Configuration*

1. On the **Point-To-Site Connectivity** page, enter the following information and then click the **Next** arrow (please read the description of Address Space in the bulleted item below). For more information about the settings on this page, see [Point-To-Site Connectivity page](http://msdn.microsoft.com/en-us/library/windowsazure/09926218-92ab-4f43-aa99-83ab4d355555#BKMK_VNETPT).

* **Address Space**, including Starting IP and CIDR (Address Count) ~ you need to make sure that this address does not conflict with the IP address range of the machine you will be connecting to on your own local network.  This address range is the IP address range that your clients will have on their PPP adapter into Azure. So first, check your client machines IP address by using ipconfig from a command prompt window.
* **Add address space**, if required for your network design.

1. On the **Virtual Network Address Spaces** page, enter the following information and then click the checkmark on the lower right to configure your network. For more information about the settings on this page, see [Virtual Network Address Spaces page](http://msdn.microsoft.com/en-us/library/windowsazure/09926218-92ab-4f43-aa99-83ab4d355555#BKMK_VNET_ADDRESS).

* **Address Space**, including Starting IP and Count. This is the address space of the Azure virtual network.
* **Add subnet**, including Starting IP and Count. Only if required for your network design. You will be required to have at least one subnet.
* **Add gateway subnet**, including Starting IP and Count. Required for this configuration. You WILL need to add a gateway subnet.  You do this by clicking on the **'Add a Gateway Subnet'** link.



*Add a Gateway Subnet*

1. After clicking the checkmark, your virtual network will begin to create. When your virtual network has been created, you will see **Created** listed under **Status** on the networks page in the Management Portal. Once your virtual network has been created, continue with the next procedure.

### Task 2 - Certificates

Certificates are used to authenticate VPN clients for point-to-site VPNs. You must generate a self- signed root certificate along with a client certificate chained to the self-signed root certificate. You can then install the client certificate on every client computer that requires connectivity.

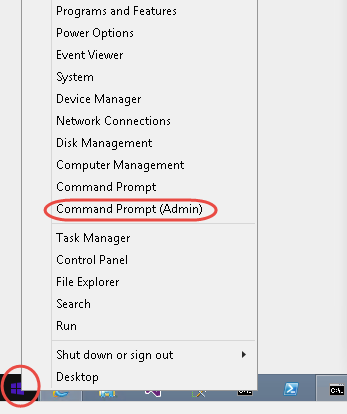
|  |
| --- |
|  |

#### [****Generate a self-signed root certificate****](javascript:void(0))

One way to create an X.509 certificate is by using the Certificate Creation Tool (makecert.exe). MakeCert is part of the [Windows SDK](http://go.microsoft.com/fwlink/?linkid=84091). For more information about using makecert, see [MakeCert](http://msdn.microsoft.com/library/windows/desktop/aa386968(v=vs.85).aspx).

For this lab exercise, you can find the MakeCert tool in the **.\Tools** subdirectory of your lab exercise files.

1. Right-click on Windows icon in the lower left hand corner of your screen and then select **Command Prompt (Admin)**.



1. Change the directory to a directory where you want to store your certificate file. On the hosted lab machine, this would be the **C:\AzureIaaSWS\Tools** directory. You will be storing your certificates in this directory and this is where you will find the MakeCert tool.
2. Type the command listed below, where **<RootCertificateName>** is the name that you want to use for the certificate. See [MakeCert](http://msdn.microsoft.com/library/windows/desktop/aa386968(v=vs.85).aspx) for more information about using this tool. NOTE: Do not include the < > brackets in your certificate name and do not name your root certificate ‘RootCertificateName’, come up with a unique name. Also, you will need to type this whole command in manually, do not copy and paste, it will not work.

***makecert -sky exchange -r -n "CN=<RootCertificateName>" -pe -a sha1 -len 2048 -ss My "RootCertificateName.cer"***

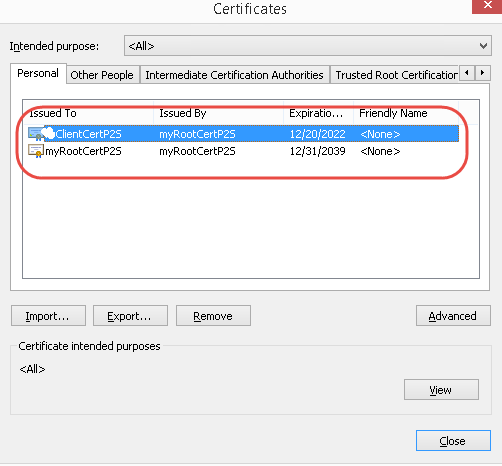
1. You will later upload the root certificate to the Microsoft Azure Management Portal.

#### [Generate the client certificate](javascript:void(0))

1. Ensure you have completed the previous steps to create a self-signed root certificate.
2. Within the same command prompt window, type the following command. NOTE: Do not include the < > brackets in your certificate name and do not name your client certificate ‘ClientCertificateName’, come up with a unique name. For the root certificate name, use the name you used in the previous task of creating the root certificate:

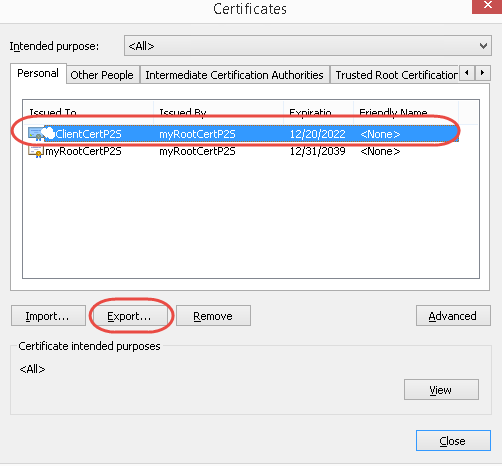
***makecert.exe -n "CN=<ClientCertificateName>" -pe -sky exchange -m 96 -ss My -in "<RootCertificateName>" -is my -a sha1***

1. All certificates are stored in your personal certificate store on your computer. Within the command prompt window, type ***certmgr.exe*** and use the certmgr UI to verify (*also located in the C:\AzureIaaSWS\Tools directory*) that the certificates are stored in the *Personal* store. You can generate as many client certificates as needed based on this procedure. It’s recommended that you create unique client certificates for each computer that you want to connect to the virtual network.



#### [Export the client certificate](javascript:void(0))

1. To export the client certificate, use certmgr.exe by using the previously opened command prompt. Select the client certificate that you want to export and then click on the **Export** button.



1. Export the **client** certificate with the private key. This will be a **.pfx** file. Make sure to record or remember the password (key) that you set for this certificate.
2. Close CertMgr.exe.

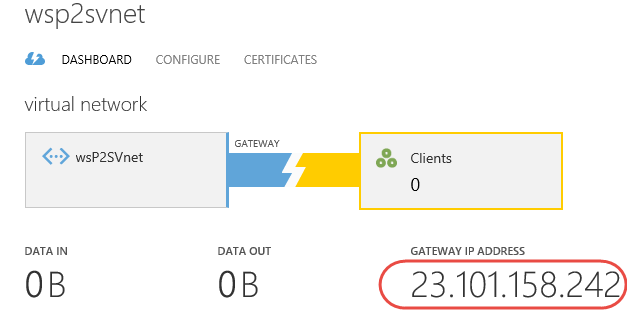
#### [Install the client certificate](javascript:void(0))

1. A client certificate must be installed on every computer that you want to connect to the virtual network. ONLY IF you are moving the client certificate to a machine that is different than the one you used in the previous steps (where you created the certificate), double-click the client certificate **.pfx** file in order to install it. Enter the password when requested. Do not modify the installation location or any other settings. Otherwise, the client certificate is already installed on your machine.
2. Once the client certificate has been installed, you can start the VPN client configuration.

### ****Task 3 - Create the dynamic routing gateway****

1. In the **Management Portal**, on the **Networks** page, click the point-to-site virtual network that you just created, and navigate to the **Dashboard** page.
2. Click **Create Gateway**, located at the bottom of the Dashboard page. A message will appear asking **Do you want to create a gateway for virtual network ‘yournetwork’**. Click **Yes** to begin creating the gateway. It could take at least 15 minutes for the gateway to be created. You have to wait for this to complete before going to the next step. Go take a break!

NOTE: Once the gateway creation has completed, you should see a screen similar to this that displays a publicly addressable IP address. This IP address is provided by Azure.



### Task 4 – Upload the root certificate

1. Upload the **root** certificate into the Virtual Network you created for the P2S network. Verify that the certificate is in .cer format and that you are uploading the root certificate and not a chained client certificate.

In the Management Portal, on the **Certificates** page for your virtual network, click **Upload a root certificate**.

1. On the **Upload Certificate** page, browse for the .cer VPN root certificate, and then click the checkmark.

|  |
| --- |
| NOTE: The certificate you will upload is the .cer root certificate, not the VPN client certificate. |

### Task 5 - Create the VPN Client configuration package

1. In the Management Portal, on the Dashboard page for your virtual network, navigate to the **quick glance** menu in the right corner and click the VPN package that pertains to the client that you want to connect to your virtual network.

The following client operating systems are supported:

* Windows 7 (32-bit and 64-bit)
* Windows Server 2008 R2 (64-bit only)
* Windows 8 (32-bit and 64-bit)
* Windows Server 2012 (64-bit only)

1. Select the download package that corresponds to the client operating system on which it will be installed:

* For 32-bit clients, select **Download x86 Client VPN Package**
* For 64-bit clients, select **Download AMD64 Client VPN Package**

It will take a few minutes to create your client package. Once the package has been completed, you will be able to download the file. The **.exe** file that you download can be safely stored on your local computer.  You may get a warning from the browser telling you that this file is not commonly downloaded and could harm your computer.  Click on the **Run** button.  If you get a warning about running the file, select **Run Anyway** and then confirm that you want to install the file.

1. Once you have finished installing the VPN client package, if you look in your Network Connections view from the Control Panel, you will see your VPN connection name.

|  |
| --- |
| NOTE: The VPN client configuration package is not signed by Microsoft. You may wish to sign the package using your organization’s signing service or sign it yourself using [SignTool](http://msdn.microsoft.com/en-us/library/windows/desktop/aa387764(v=vs.85).aspx). It’s OK to use the package without signing. However, if the package isn’t signed, a warning will appear when you install the package. |

### Task 6 - Start the VPN Connection

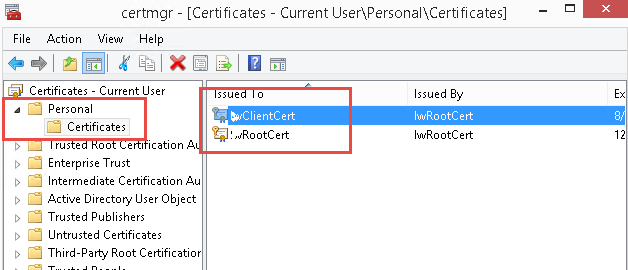
1. On the client computer, navigate to VPN connections, locate the VPN connection for your virtual network, and click **Connect**.

A pop up message will appear which is used to create a self-signed cert for the Gateway endpoint. Click **Continue** to use elevated privileges.

1. On the **Connection** status page, click **Connect** in order to start the connection.
2. On the **Select Certificate** screen, verify that the client certificate showing is the one that you want to use to connect. If it is not, use the dropdown arrow to select the correct certificate, and then click **OK**.
3. You are now connected to your virtual network and have full access to any service or virtual machine hosted in your virtual network.

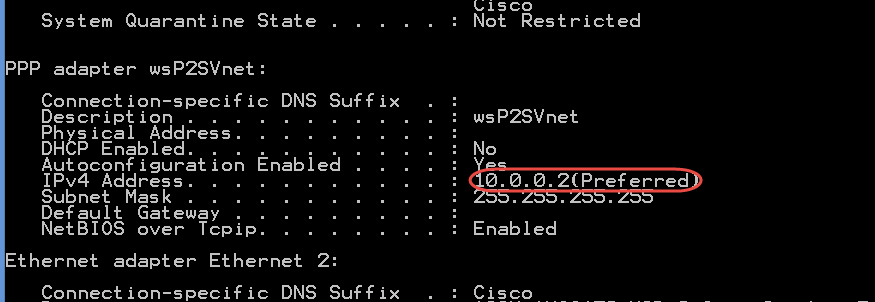
NOTE: If you receive certificate error problems when you try to connect via your VPN, perform the following verification using certmgr.msc. You can do this by typing in certmgr.msc into the Command Prompt window (opened as administrator):

* Verify that the root and client certificate is in the ***My store*** personal store. For example: ***Certificates - Current User/Personal/Certificates***.



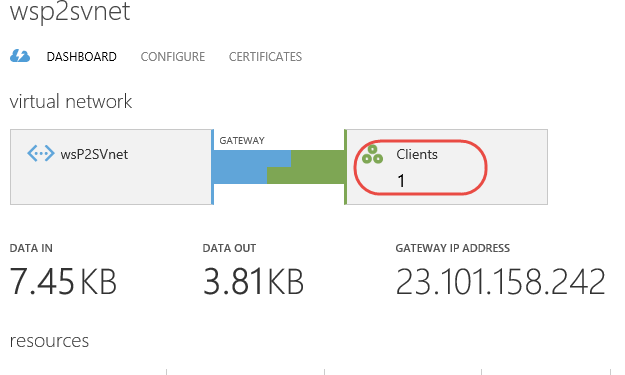
### Task 7 - Verify the VPN Connection

1. To verify that your VPN connection is active, open an elevated command prompt, and run **ipconfig/all** on the local computer that you are connecting to Azure with.
2. View the results. The results should show something similar to this. This is the IP address that the virtual network sees the on-premises machine as.  Therefore, if you need to connect to something on the on-premises machine from Azure, this is the address you will use.



Also notice that this IP address came from the IP address range that we selected when we were stepping through the wizard on the Point-to-Site connectivity page.

If you go back into the management portal to the virtual network dashboard page, after a few minutes you will be able to confirm that a client is connected.



## Summary

By completing this hands-on lab you have learned how to:

* Configure a new virtual network with a Point-to-Site configuration.