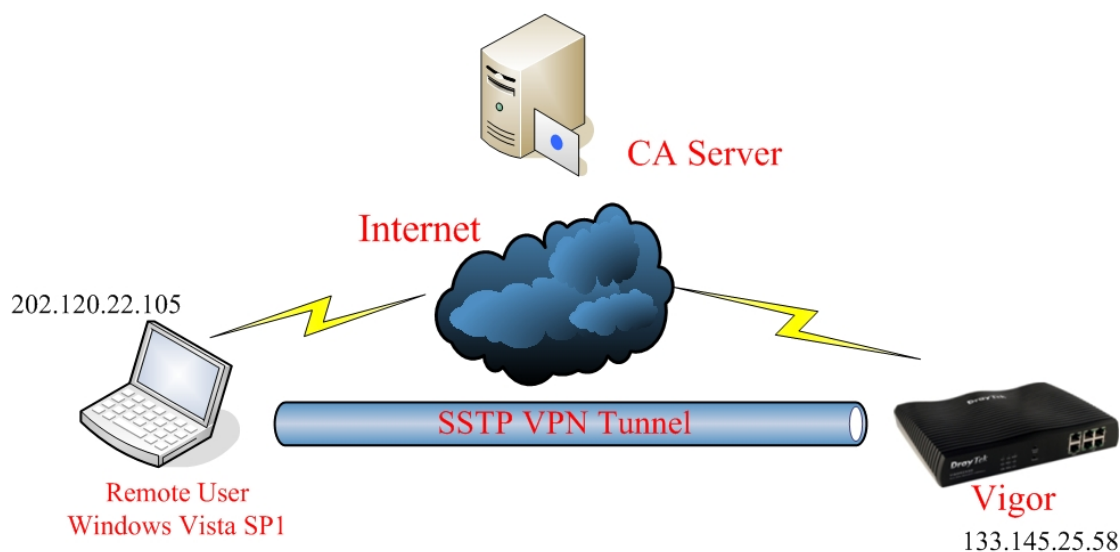


How to Connect SSTP VPN from Windows Server 2008/Vista to Vigor2950



Requirements

- Windows Server 2008, or Windows Vista SP1
- Local Certificate (a online CA server on the Internet is required for some situation which may be described below)
- Vigor 2950 Series (acted as SSTP server)

Configure Vigor Router Settings

This section introduces how to configure the Vigor router as an SSTP VPN server.

1. Make sure the router has obtained the right time. Otherwise there might be troubled in certificate authentication.

System Maintenance >> Time and Date

Time Information

Current System Time	2008 Sep 18 Thu 6 : 21 : 1	Inquire Time
---------------------	----------------------------	--------------

Time Setup

<input type="radio"/> Use Browser Time	
<input checked="" type="radio"/> Use Internet Time Client	
Time Protocol	NTP (RFC-1305) ▼
Server IP Address	pool.ntp.org
Time Zone	(GMT) Greenwich Mean Time : Dublin ▼
Enable Daylight Saving	<input type="checkbox"/>
Automatically Update Interval	30 min ▼

OK Cancel

2. Configure the certificate management. For configuring SSTP VPN, there are three types of certificates that can be used in Vigor routers. Please import one of the three types of certificates for your necessity.

Certificate Management >> Local Certificate

Import X509 Local Certificate

Upload Local Certificate
Select a local certificate file.
Certificate file: No file chosen
Click [Import](#) to upload the local certificate.

Upload PKCS12 Certificate
Select a PKCS12 file.
PKCS12 file: No file chosen
Password:
Click [Import](#) to upload the PKCS12 file.

Upload Certificate and Private Key
Select a certificate file and a matchable Private Key.
Certificate file: No file chosen
Key file: No file chosen
Password:
Click [Import](#) to upload the local certificate and private key.

3. Next, in the menu **SSL VPN >> General Setup**, choose the certificate that you just uploaded as the **Server Certificate**.

SSL VPN >> General Setup

SSL VPN General Setup

Port (Default: 443)
Server Certificate
Encryption Key Algorithm
☐ High - AES(128 bits) and 3DES
☒ Default - RC4(128 bits)
☐ Low - DES

Note: The settings will act on all SSL applications.

Brief Introduction for the Certificates

Vigor routers allow you to generate a certificate request and submit it to the CA server, and later import it as a Local Certificate. If you have already gotten a certificate from a third party, you can import it directly. Besides, the router can also support types such as PKCS12 Certificate and Certificate with a Private Key. They are introduced respectively below.

- **Local Certificate** - In this section, we mainly discuss how to generate a certificate request by the Vigor router, and how to submit it to the CA server, get a newly issued certificate and import it to the router.

Request a new certificate

- From the router's web configurator, please open **Certificate Management >> Local Certificate**. Next, click the **Generate** on the bottom of the page.

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
---	---	---	View	Delete
---	---	---	View	Delete
---	---	---	View	Delete

- The page of Generate Certificate Signing Request will display as follows. You can input the detailed information of this certificate. **Note that Common Name should be configured with the SSTP server's WAN IP or domain name, otherwise you'll encounter authentication problem when connecting the SSTP VPN.**

Certificate Management >> Local Certificate

Generate Certificate Signing Request

Certificate Name	<input type="text" value="draytekdemo"/>
Subject Alternative Name	
Type	<input type="text" value="IP Address"/>
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text" value="Draytek"/>
Organization Unit (OU)	<input type="text" value="Draytek Sales"/>
Common Name (CN)	<input type="text" value="10.1.1.254"/>
Email (E)	<input type="text"/>
Key Type	<input type="text" value="RSA"/>
Key Size	<input type="text" value="1024 Bit"/>

- Click **Generate**. You will return to the local certificate list page. The certificate that you've just configured will be displayed with status "Requesting".

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

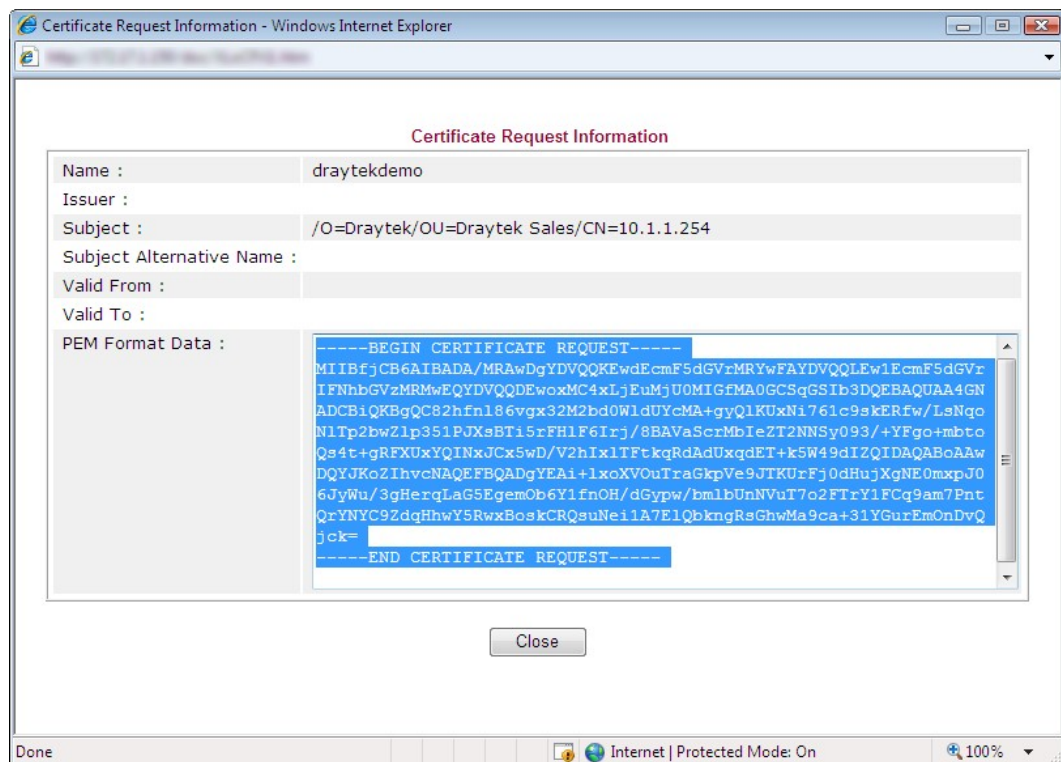
Name	Subject	Status	Modify	
draytekdemo	/O=Draytek/OU=Draytek Sales/...	Requesting	View	Delete
---	---	---	View	Delete
---	---	---	View	Delete

GENERATE

IMPORT

REFRESH

- iv. Click **View**. Copy the certificate request information from the window.



- v. Access your CA server and enter the page of certificate request. Copy the information to it and submit a request. Then, a new certificate will be issued to you by the CA server. Please save it properly.

Import the certificate

- i. Open **Certificate Management >> Local Certificate**, and click **Import**.
- ii. In the page of **Import X509 Local Certificate**, importing local certificate - the one that is saved previously.

Import X509 Local Certificate

Upload Local Certificate

Select a local certificate file.

Certificate file: D:\Users\draytek\Desktop\NewCert.c

Click **Import** to upload the local certificate.

Upload PKCS12 Certificate

Select a PKCS12 file.

- iii. If you have done well in the above procedure, you will see the following page.

Import X509 Local Certificate

Congratulation!

Local Certificate has been imported successfully.

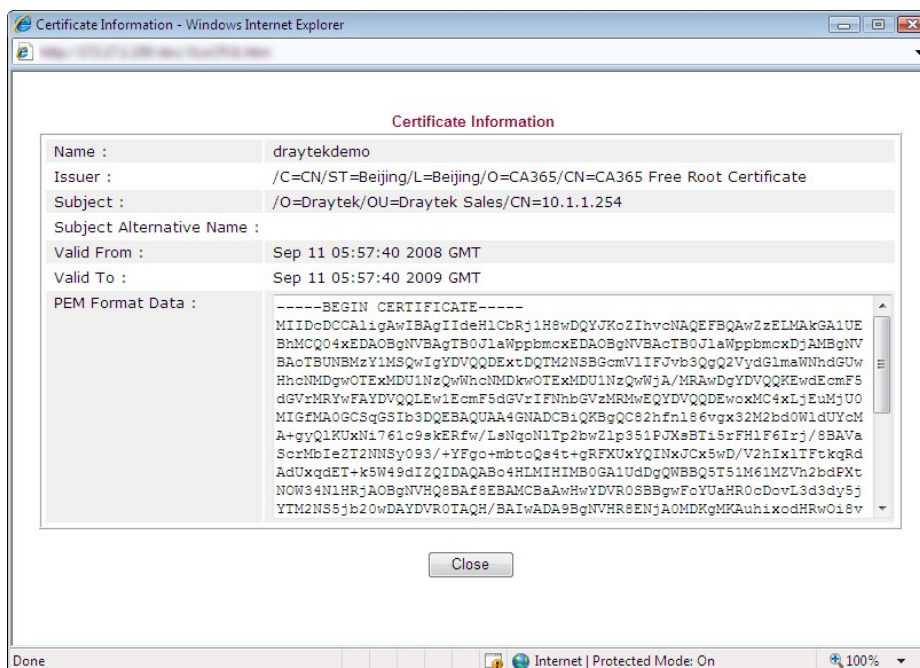
Please click to view the certificate.

- iv. Now, the **Status** for your certificate will display **OK**.

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

- v. You can view the details of the issued certificate by clicking "view":



- **PKCS12 Certificate** - If you get a PKCS12 certificate from a third party, you may import to the router as the certificate for SSTP VPN as well. Choose the certificate file, and type the password. Then start to import.

Upload PKCS12 Certificate

Select a PKCS12 file.

PKCS12 file: certificate.pfx

Password:

Click **Import** to upload the PKCS12 file.

- **Certificate with Private Key** - If you get a certificate together with a private key file from a third party, you may import it to the router as the certificate for SSTP VPN as well. Choose the certificate file, and type the password. Then start to import.

Upload Certificate and Private Key

Select a certificate file and a matchable Private Key.

Certificate file: certificate.pem

Key file: private key file.key

Password:

Click **Import** to upload the local certificate and private key.

Configure Client settings

This section introduces how to configure settings for the client with Windows Server 2008/Vista SP1 to connect the SSTP VPN server as a remote dial-in user.

A. Add Trusted Root Certificate

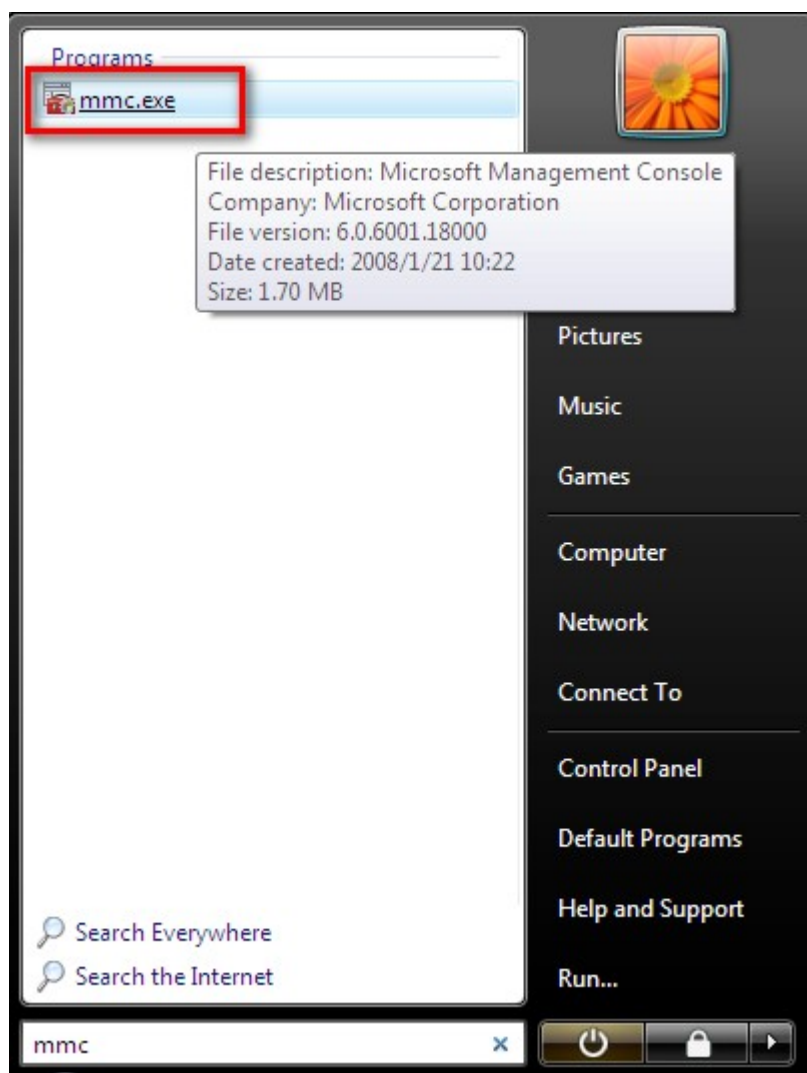
Such step can make the authentication procedure being completed successfully when connects to VPN server via SSTP.

Note: First, get the "Trusted Root Certificate" ready.

If you have generated the certificate request via the Vigor router and submitted it to a CA server, please download and save the Root Certificate from the CA server; or if you have imported a third-party certificate, you must have a Root Certificate together with that.

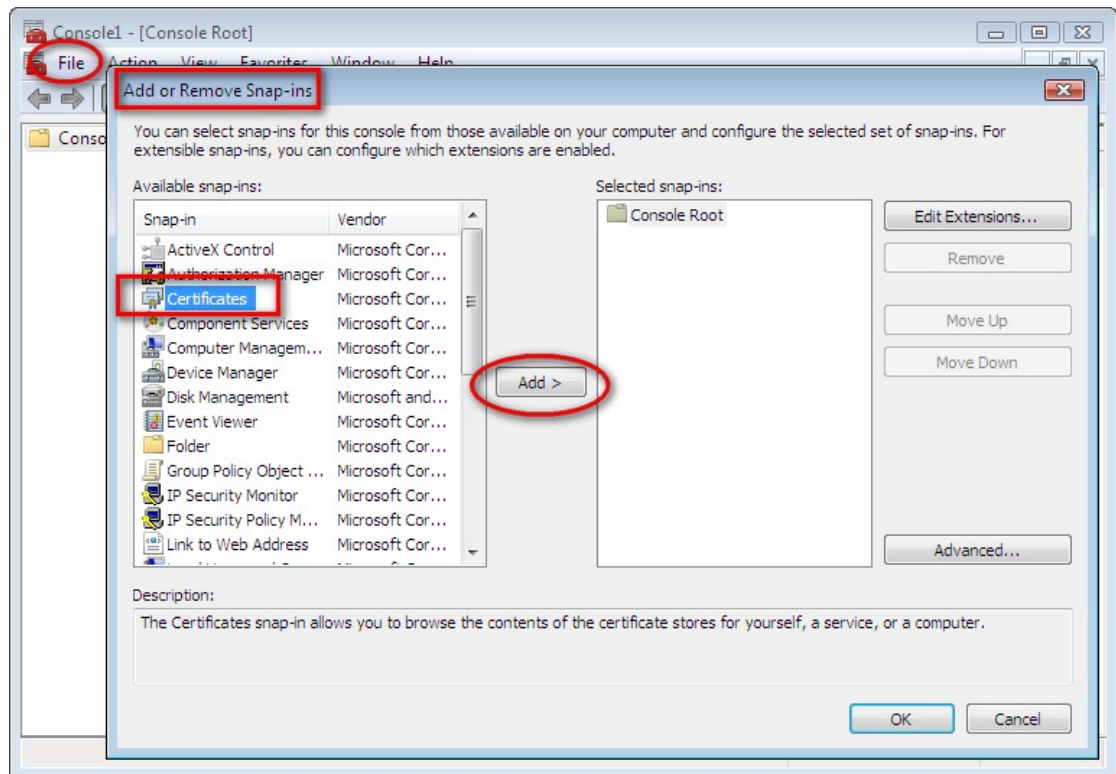
Make sure you have the Trusted Root Certificate in your computer, and do the following:

1. Enter the **Console** of the Windows System:

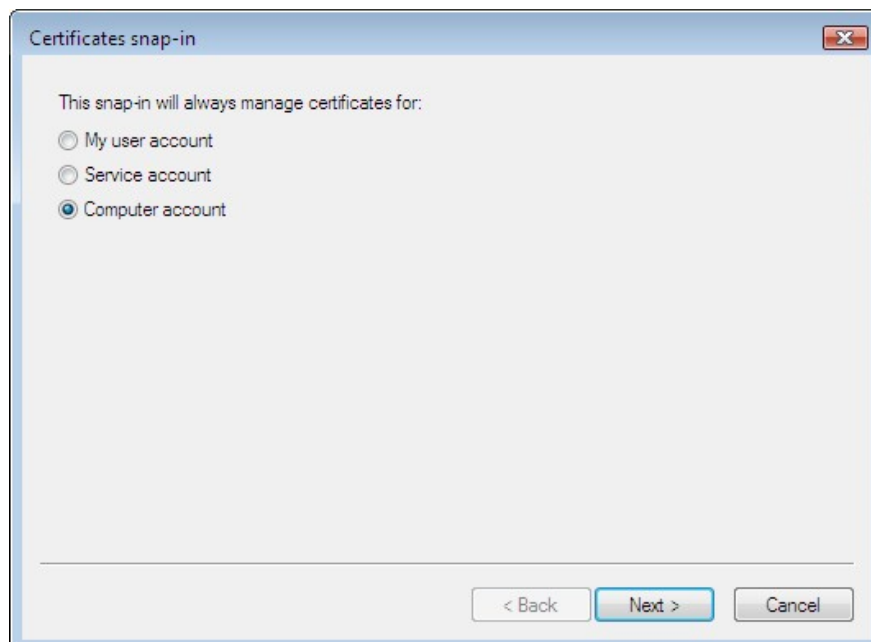


2. Different from the method above, you can also click "Start" and then "Run", and input "mmc.exe" and press Enter to get the Console window.

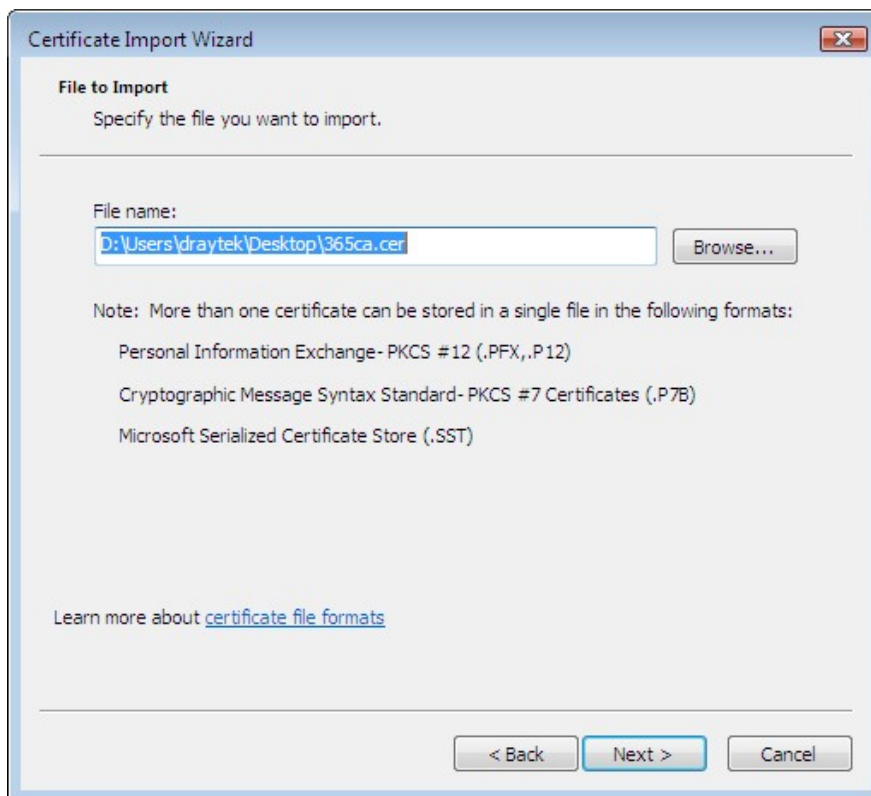
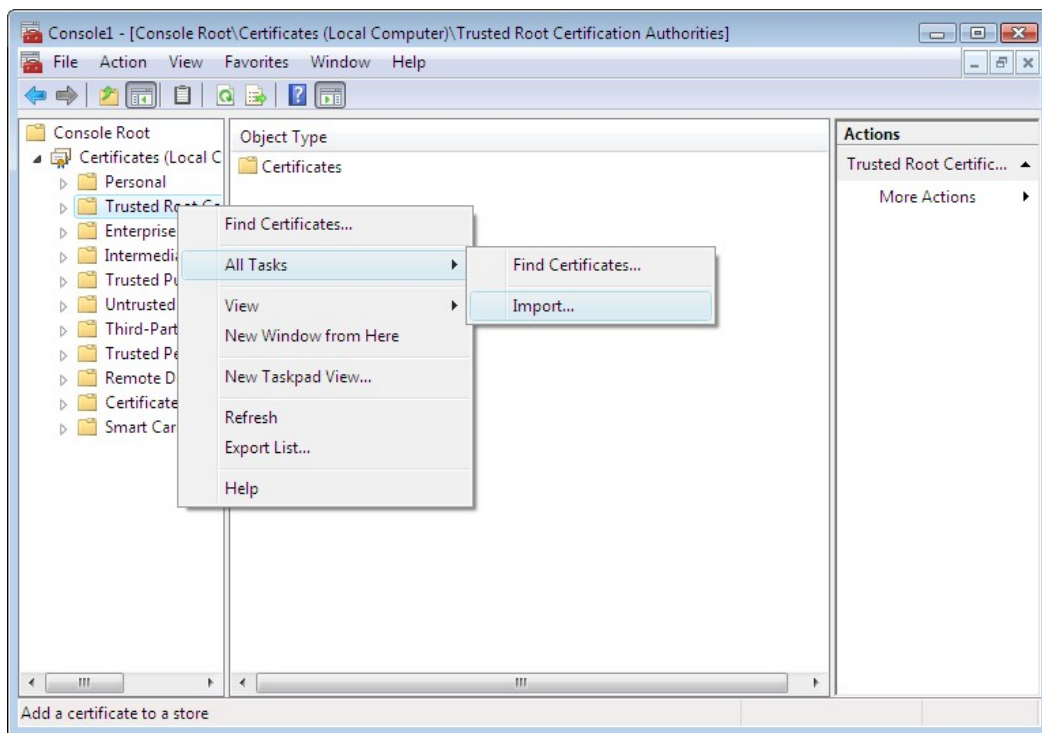
3. In the Console window, click File menu and choose to "Add or Remove Snap-ins". Select "Certificate" and add it.



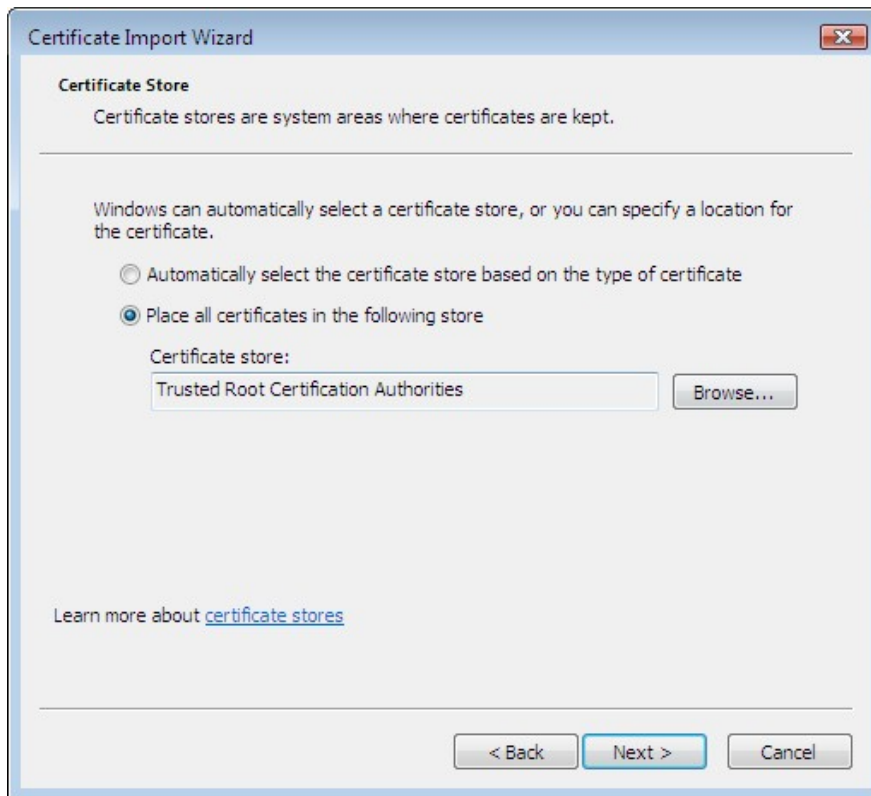
4. Beware to choose **Computer account** but not a **My user account**. Otherwise it might cause problems in SSTP certificate authentication.



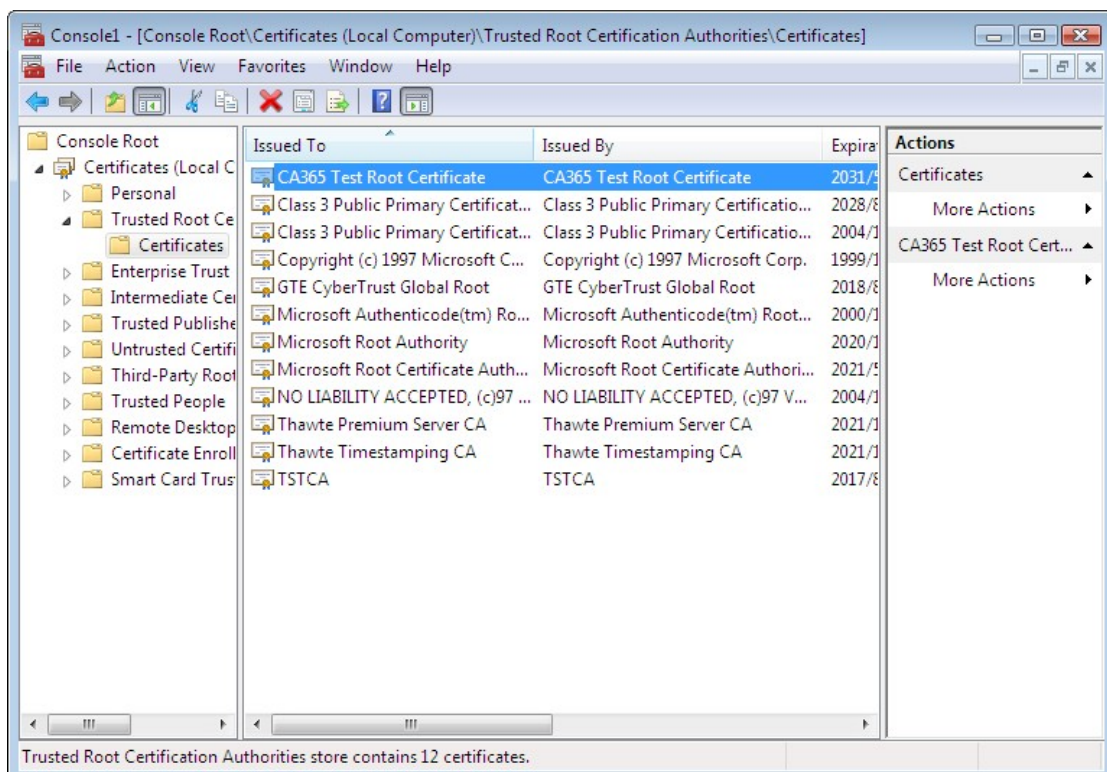
5. In the new-added Certificate folder, right click on **Trusted Root Certificate** and choose **All Tasks>>Import**.



6. Choose the **Trusted Root Certificate** that you saved in local place, and import it to **Trusted Root Certificate**. Then, click **Next**.



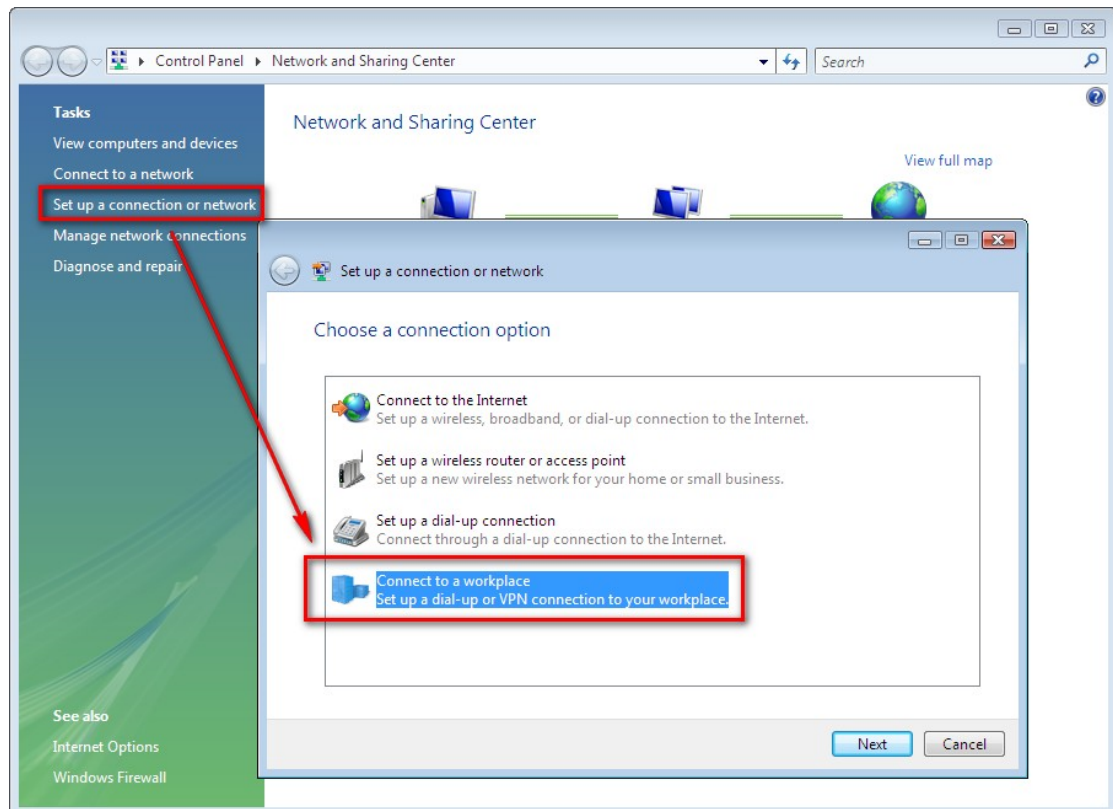
7. You can check if it has been successfully added.



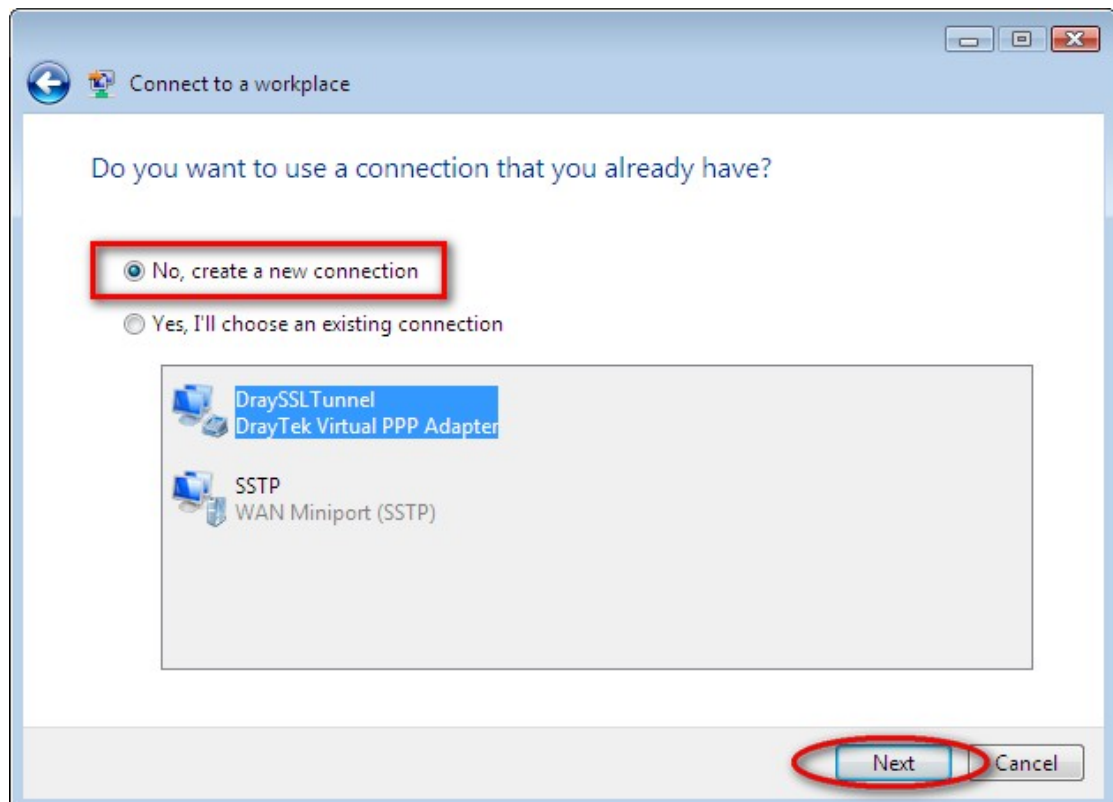
B. Configure Windows Built-in VPN Client Setup

VPN Client for SSTP mode has been merged into Vista SP1. Users can easily configure it and dial the Vigor SSTP VPN server by following the instructions listed below:

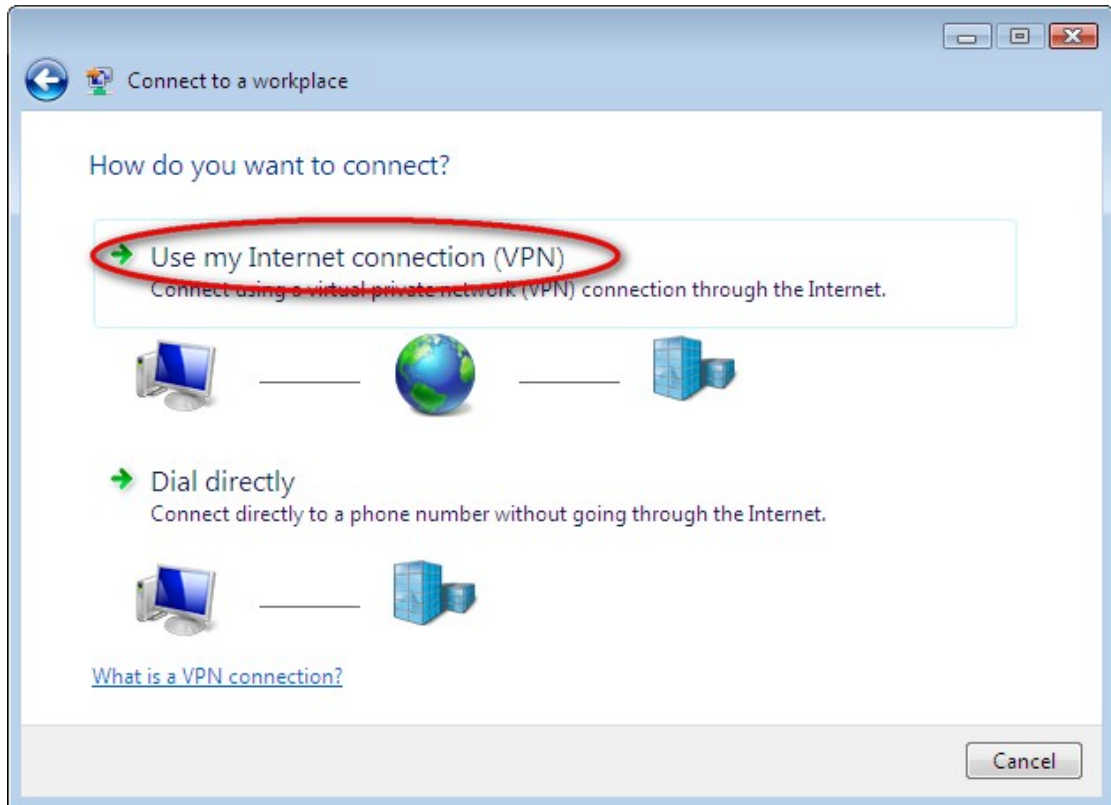
1. Choose **Connect to a workplace**, and then click **Next** to build a new connection:



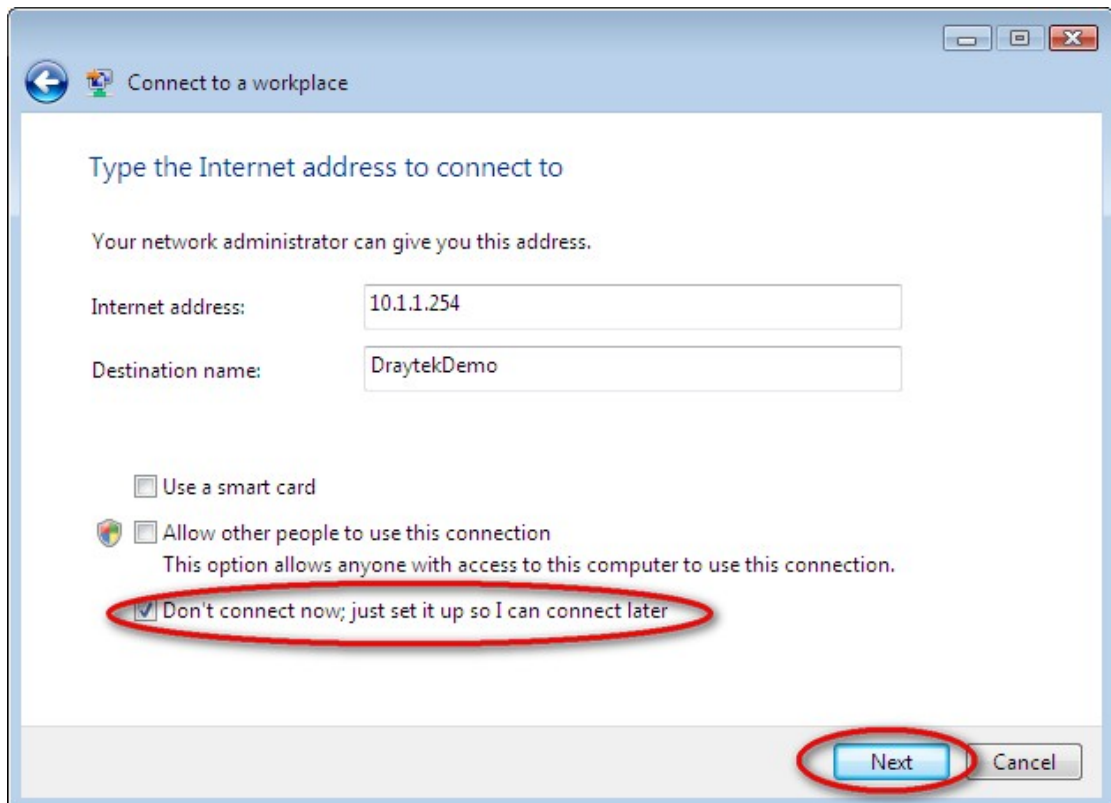
2. In this page, please choose **No, create a new connection** and click **Next**.



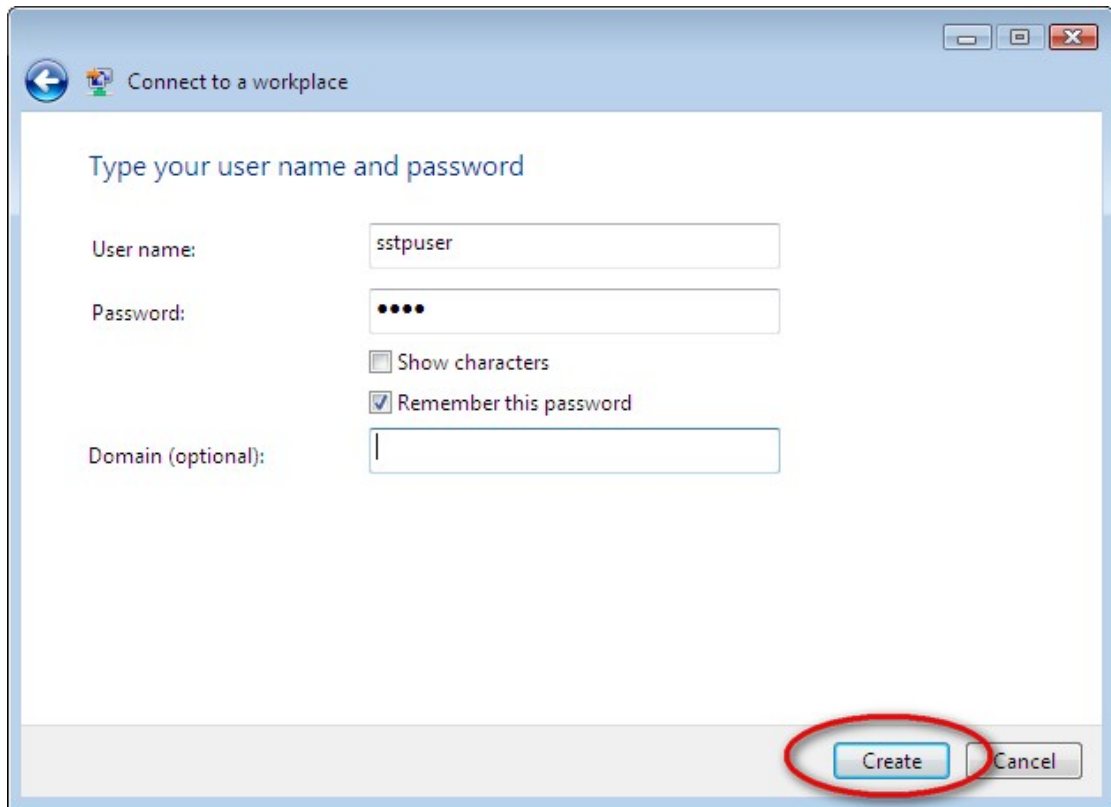
3. In the following page, click **Use my Internet connection (VPN)**.



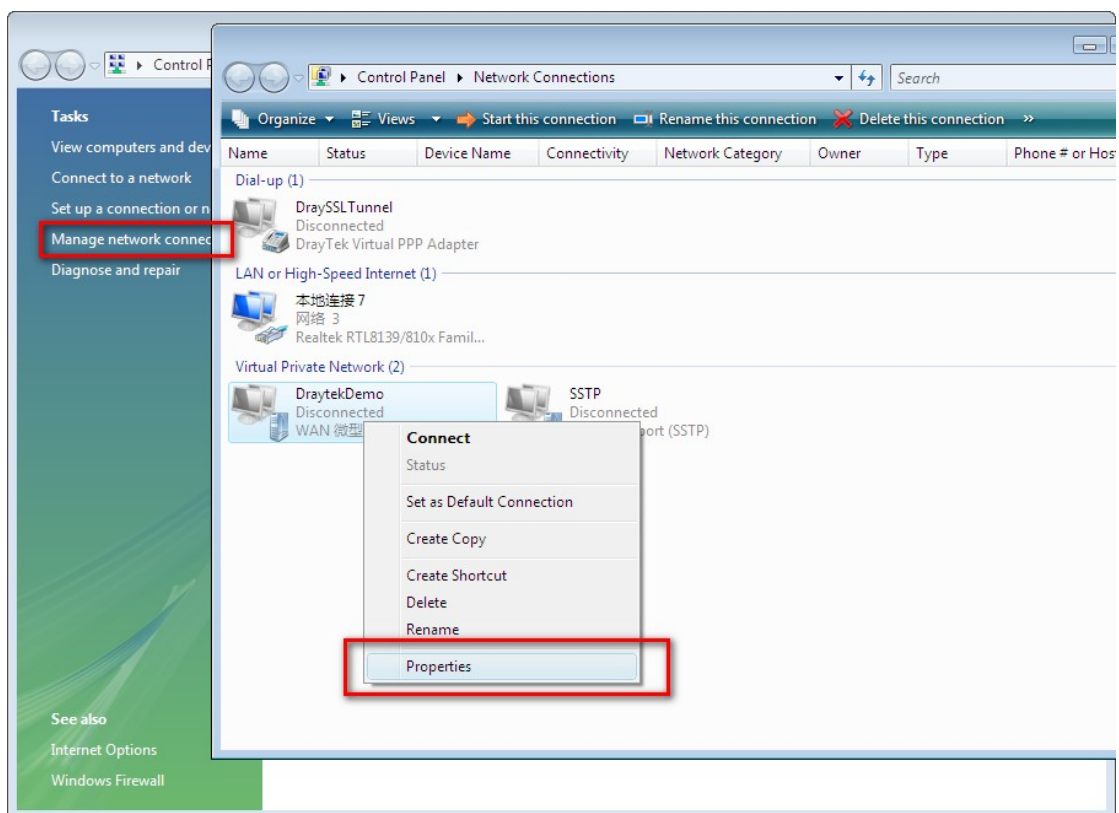
4. On the following page, type the Internet Address of the VPN server (IP Address or domain name) and destination name. Select **Don't connect now.....** and click **Next**.



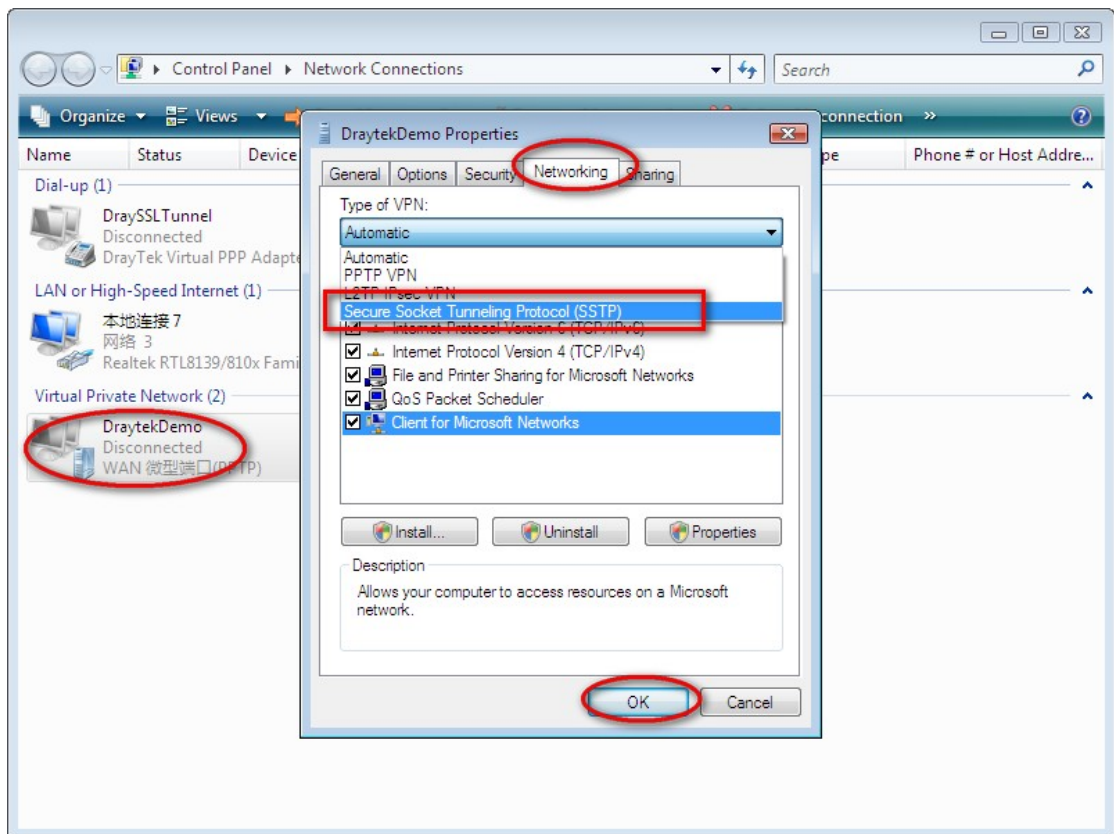
5. Type the username and password, and click **Create**.



6. Go back to **Manage network connections** and find the VPN connection that you have just created (e.g, DraytekDemo). Right click on it and choose **Properties**.



7. In the pop-up dialog box, click the **Networking** tab and choose **Secure Socket Tunneling Protocol (SSTP)**. Click **OK** to finish the configuration for dialing a SSTP VPN tunnel:



8. Finally, double click **DraytekDemo** to open the following dialog. Type the username and password here to execute a SSTP VPN connection.

