

Connect anywhere with OpenVPN and Tomato

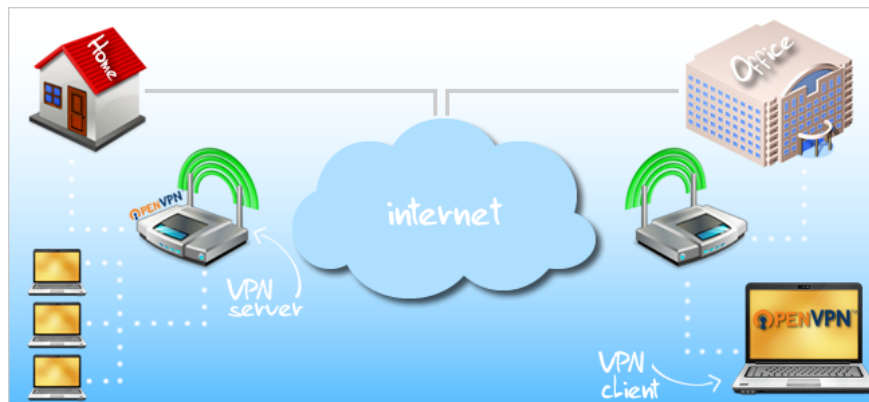
Today we will continue to exploit Tomato firmware features through installing OpenVPN with Tomato, then setting up to access the network anywhere in the world.

Wear Management - In the previous article we showed you how to install and tips on using Tomato, an open source firmware for routers on the Linksys WRT54GL. Today we will continue to exploit the features of this firmware by installing OpenVPN with Tomato, then setting up to be able to access the network anywhere in the world.

>>>Enhance OpenVPN security with One Time Password on Ubuntu



What is OpenVPN?



Basically, a VPN is a private network that uses a public network (usually the Internet) to connect remote locations or users to a LAN at the central office. Instead of using a rather complex connection like a digital subscriber line, VPN creates virtual links that are transmitted over the Internet between an organization's private network with a remote location or user.

Virtual Private Network (VPN) is a very secure, reliable connection between a local area network (LAN) and another system. You can imagine your router as a bridge to connect the network. Your computer and the OpenVPN server (in this case the router itself) will " *shake hands* " with each other using a certificate of mutual affirmation. After confirmation, both the client and server will agree to ' *trust* ' each other and allow access to the server's network.

Usually, deploying VPN software and hardware is time-consuming and costly, so **OpenVPN** is a completely free open source VPN solution. Tomato with OpenVPN is now considered the most perfect solution for those who want a secure connection between two networks without any extra cost. However, the default of OpenVPN does not work as expected. So we need to tweak and reconfigure it a bit. Here are the steps to take:

Request

To do this tutorial we need a computer running Windows 7 with an admin account. If you are using Mac or Linux, this guide will also help you understand its performance, but you need to do more research to be most effective for yourself.

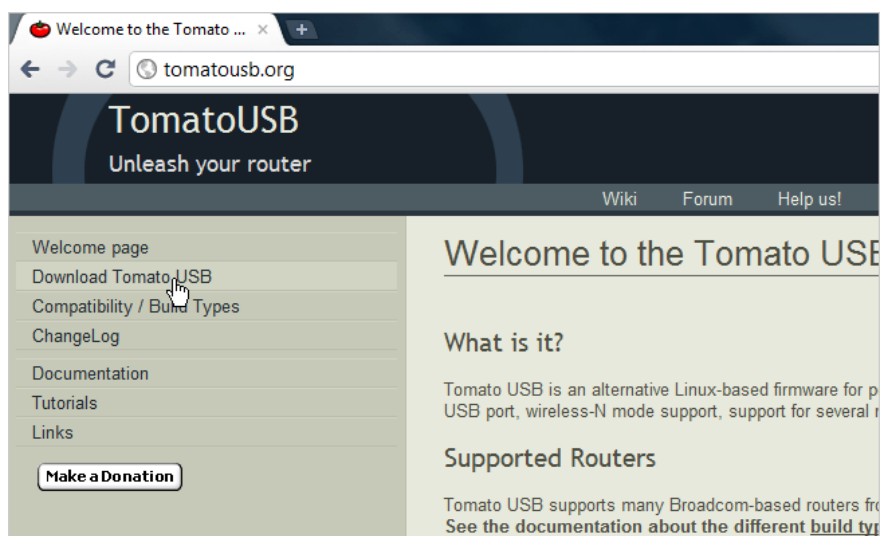
We will install a special version of Tomato called **TomatoUSB VPN** on the *Linksys WRT54GL* version 1.1 router. To check if your router is compatible with TomatoUSB, please go to the TomatoUSB Build page to see it.

Before we start we need to install the original firmware on the router or Tomato firmware that we described in the previous article.

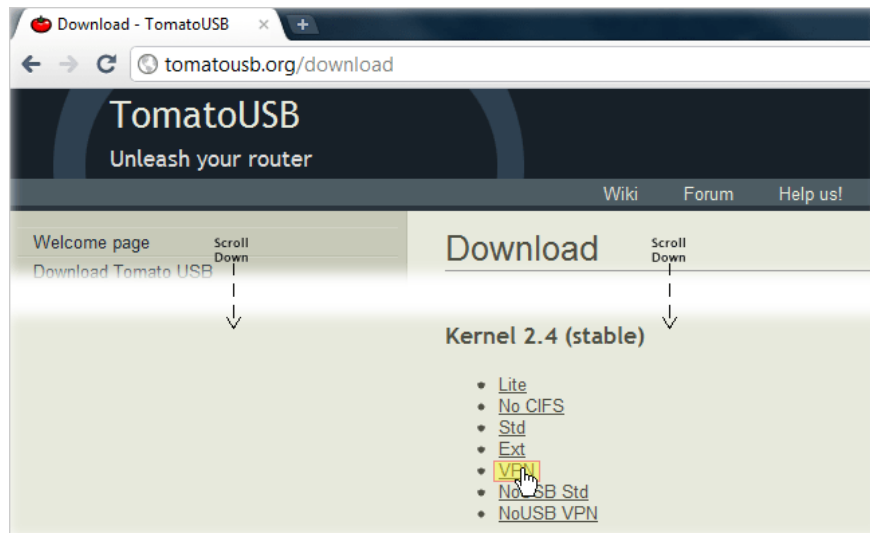
Install TomatoUSB

In the previous tutorial, we installed the Tomato v1.28 firmware from *PolarCloud* 's website. However, this version does not support OpenVPN, so we need to install a new version called **TomatoUSB VPN** .

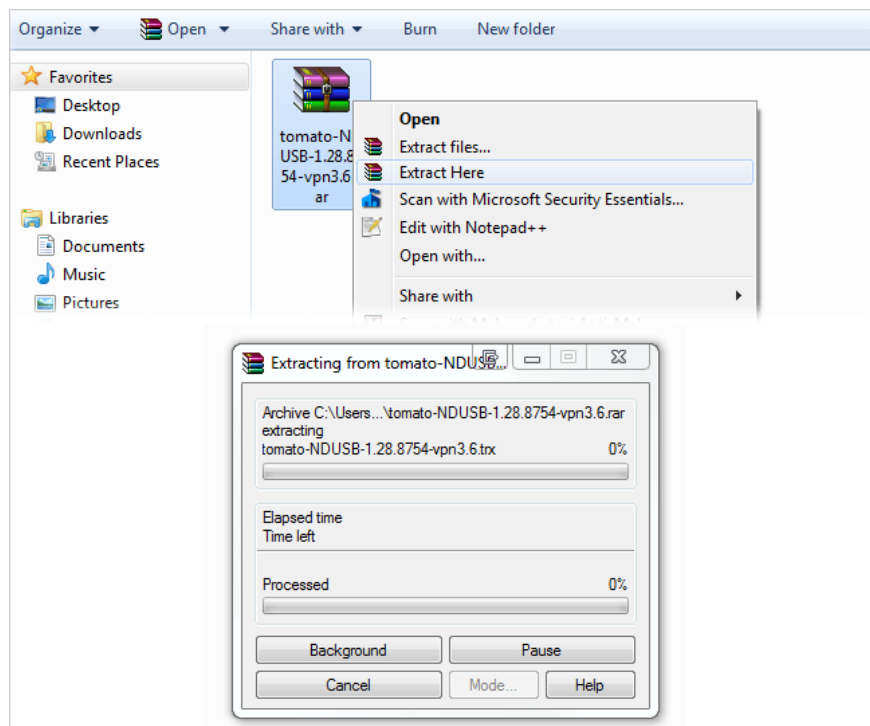
First go to TomatoUSB's homepage and click the **Download Tomato USB link** to download.



Scroll to the bottom of the page, in the **Kernel 2.4 (stable)** section, click the **VPN** link to download your file with the **.rar file** .



Then you use the decompression program (like WinRAR) to extract the downloaded file. You will receive two files, **CHANGELOG** and **tomato-NDUSB-1.28.8754-vpn3.6.trx** .



1. Where the router is running Linksys firmware

Open your browser and enter the IP address (default is *192.168.1.1*). Enter ' *admin* ' for both " *username* " and " *password* " fields when requested.

LINKSYS by Cisco Firmware Version: v4.30.15

Wireless-G Broadband Router WRT54GL

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Setup | DNS | MAC Address Clone | Advanced Routing

Language
Select your language: English

Internet Setup
Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some ISPs)

Router Name: WRT54GL
Host Name:
Domain Name:
MTU: Auto
Size: 1500

Network Setup
Router IP

Local IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

Network Address Server Settings (DHCP)

DHCP Server: Enable Disable
Starting IP Address: 192.168.1.100
Maximum Number of DHCP Users: 50
IP Address Range: 192.168.1.100 to 149
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0.0.0.0
Static DNS 2: 0.0.0.0

Automatic Configuration - DHCP: This setting is most commonly used by Cable operators.
Host Name: Enter the host name provided by your ISP.
Domain Name: Enter the domain name provided by your ISP.
Local IP Address: This is the address of the router.
Subnet Mask: This is the subnet mask of the router.
DHCP Server: Allows the router to manage your IP addresses.
Starting IP Address: The address you would like to start with.
Maximum number of DHCP Users: You may limit the number of addresses your router hands out.

Login successfully, click the **Administration > Firmware Upgrade** menu .

LINKSYS by Cisco Firmware Version: v4.30.15

Wireless-G Broadband Router WRT54GL

Administration Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Management | Log | Diagnostics | Factory Defaults | **Firmware Upgrade** | Configuration Management

Router Password
Local Router Access

Router Password:
Re-enter to confirm:

Web Access

Access Server: HTTP HTTPS
Wireless Access Web: Enable Disable

Remote Router Access

Remote Management: Enable Disable
Management Port: 8080
Use https:

UPnP

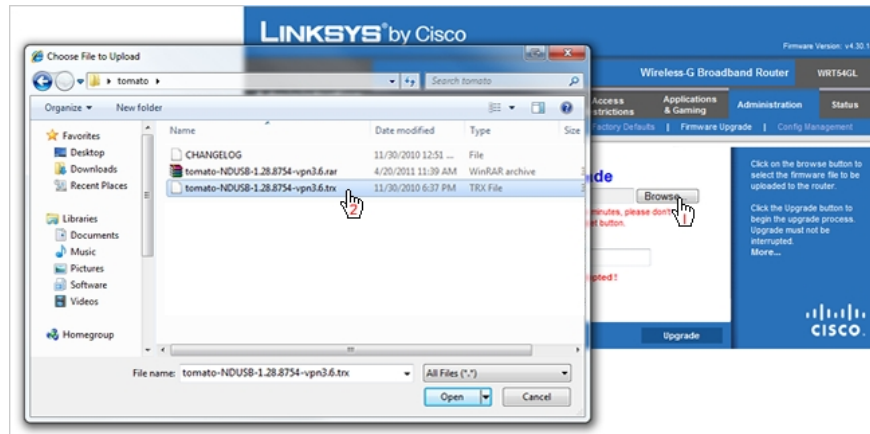
UPnP: Enable Disable
Allow Users to Configure: Enable Disable
Allow Users to Disable Internet Access: Enable Disable

Local Router Access: You can change the Router's password from here. Enter a new Router password and then type it again in the Re-enter to confirm field to confirm.
Web Access: Allows you to configure access options to the router's web utility.
Remote Router Access: Allows you to access your router remotely. Choose the port you would like to use. You must change the password to the router if it is still using its default password.
UPnP: Used by certain programs to automatically open ports for communication.

Save Settings **Cancel Changes**

Click the **Browse** button and navigate to the extracted TomatoUSB file, select the *tomato-NDUSB-1.28.8754-vpn3.6.trx* file , then click the **Upgrade** button on the browser interface.

Your router will start installing TomatoUSB VPN, this process takes a few minutes to complete. After the update process finishes, open the *command prompt* dialog box and enter **ipconfig –release** to redefine the new IP address for the router, then type **ipconfig –renew** to give it a new address. The numbers next to the **Default Gateway** line will be the router's new IP address.



Note: After installing Tomato, go to **Administration > Configuration** and select 'Erase all NVRAM . '.

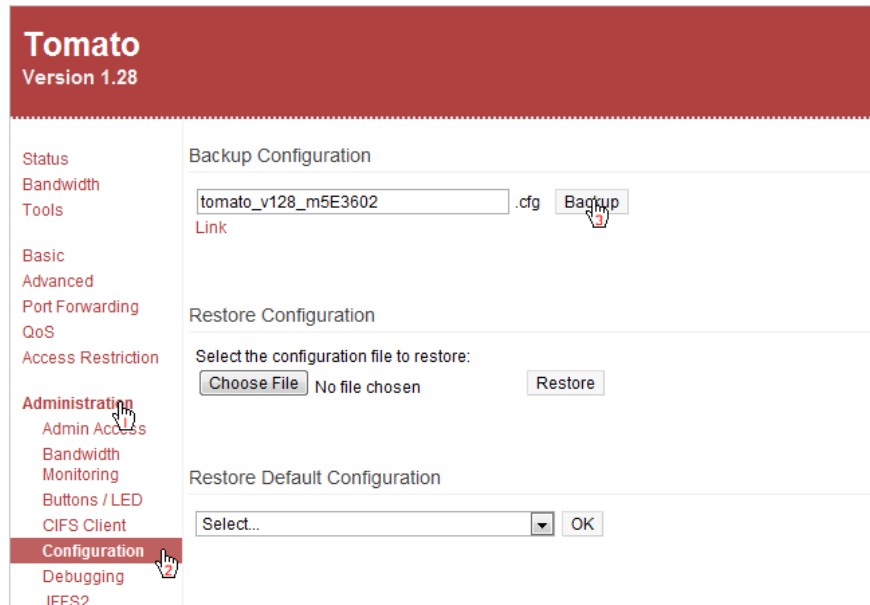
2. If the router is running Tomato firmware

Open your browser and enter that IP address and then log in as above.

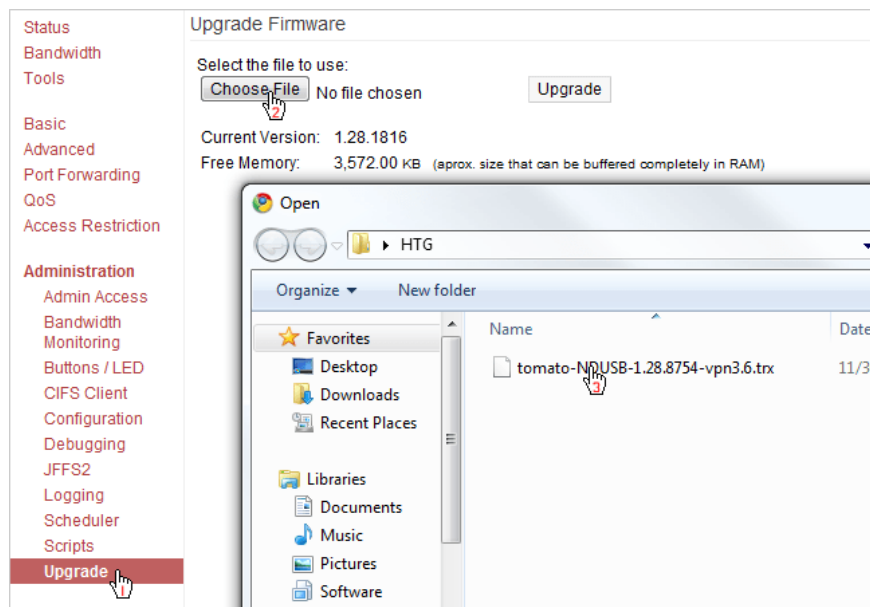
A screenshot of the Tomato Version 1.28 web interface. The interface is divided into several sections: Status, System, WAN, and LAN. The System section shows the router's name (WRT54GL), model (Linksys WRT54G/GS/GL), and system time (Tue, 12 Apr 2011 00:41:01 -0700). The WAN section shows the MAC Address (00:25:9C:5E:36:03), Connection Type (DHCP), IP Address, Subnet Mask (255.255.255.0), Gateway, DNS, and MTU (1500). The LAN section shows the Router MAC Address (00:25:9C:5E:36:02), Router IP Address (192.168.1.1), Subnet Mask (255.255.255.0), and DHCP range (192.168.1.100 - 192.168.1.149).

Tomato Version 1.28		WRT54GL
Status	System	
Overview	Name	WRT54GL
Device List	Model	Linksys WRT54G/GS/GL
Logs	Time	Tue, 12 Apr 2011 00:41:01 -0700
Bandwidth	Uptime	0 days, 00:05:14
Real-Time	CPU Load (1 / 5 / 15 mins)	0.03 / 0.03 / 0.00
Last 24 Hours	Total / Free Memory	14.19 MB / 6,008.00 KB (41.35%)
Daily	WAN	
Weekly	MAC Address	00:25:9C:5E:36:03
Monthly	Connection Type	DHCP
Tools	IP Address	
Basic	Subnet Mask	255.255.255.0
Advanced	Gateway	
Port Forwarding	DNS	208.59.247.45:53, 208.59.247.46:53
QoS	MTU	1500
Access Restriction	Status	Connected
Administration	Connection Uptime	0 days, 00:05:05
About	Remaining Lease Time	6 days, 23:54:55
Reboot...	<input type="button" value="Renew"/> <input type="button" value="Release"/>	
Shutdown...	LAN	
Logout	Router MAC Address	00:25:9C:5E:36:02
	Router IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	DHCP	192.168.1.100 - 192.168.1.149

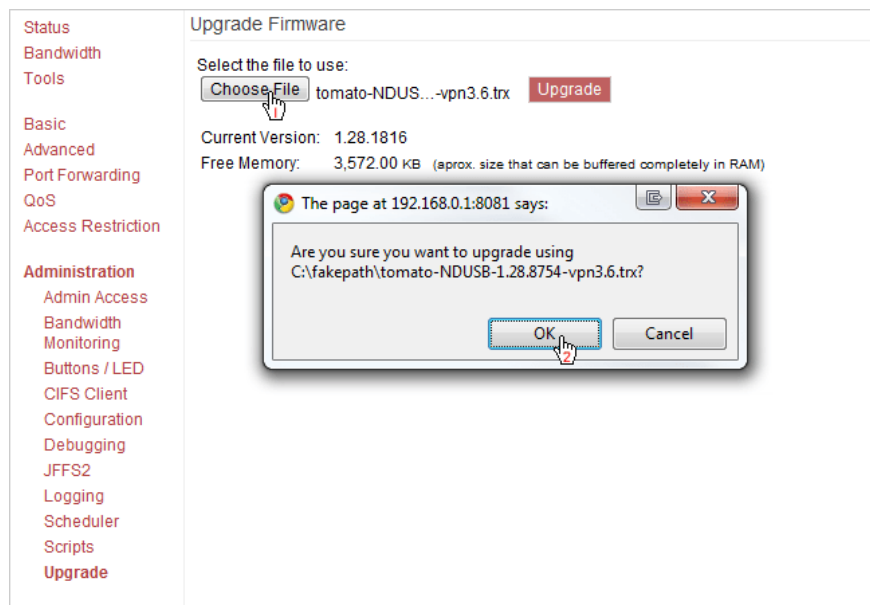
Although it is not necessary, you can also back up the Tomato configuration before proceeding to upgrade to TomatoUSB VPN. To save the configuration, go to **Administration** > **Configuration** and click **Backup** . This will ask you to save a file in **.cfg** format on your computer.



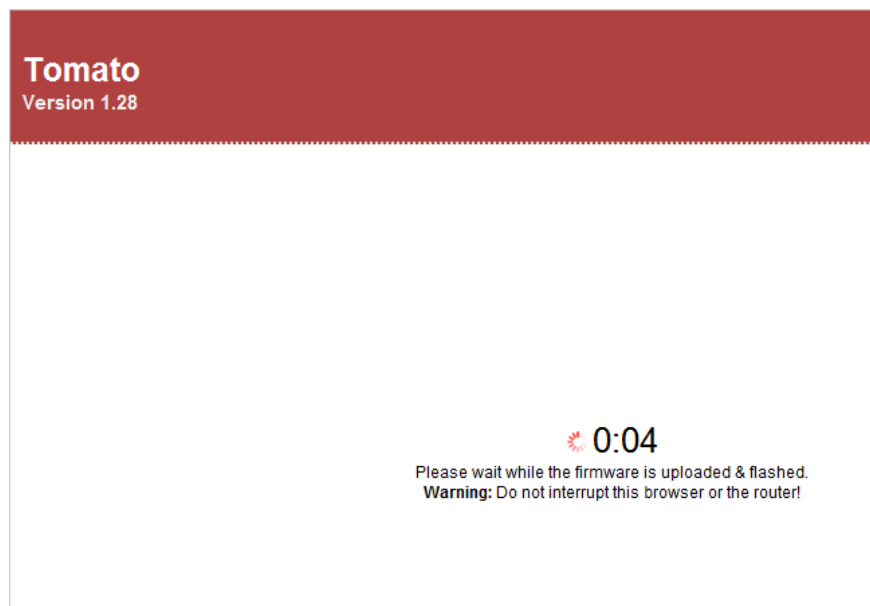
Now is the time to start upgrading Tomato to TomatoUSB VPN. Under **Administration** menu select **Upgrade** , then click **Choose File** button, navigate to the unzipped folder and select *tomato-NDUSB-1.28.8754-vpn3.6.trx* . Press **Upgrade** .



The dialog box asks for confirmation of upgrade, press **OK** .



Wait a few minutes for the router to update and restart automatically.



After restarting, you will probably get another IP address. In our case, the IP address remains the same. To determine the IP address, open the command prompt and type **ipconfig –release** , then **ipconfig –renew** and look at the **Default Gateway** line.

If your configuration is returned to the default, go to the **Configuration** page (*Administration > Configuration*) and click the **Choose File** button under *Restore Configuration* . Find the **.cfg** file you just saved in the previous step and click **Restore** .

Configure OpenVPN

After upgrading to TomatoUSB VPN, at Tomato interface, there will be a new menu, *Web Usage, USB and NAS* , and *VPN Tunneling* . In this example we are only interested in the **VPN Tunneling** menu, click it and keep the browser open and go to the next step.

Tomato	
Version 1.28	
Status	System
Overview	Name: The Tomato
Device List	Model: Linksys WRT54G/GS/GL
Web Usage	Time: Wed, 20 Apr 2011 14:01:04 -0500
Logs	Uptime: 0 days, 12:19:36
Bandwidth	CPU Load (1 / 5 / 15 mins): 0.00 / 0.00 / 0.00
Tools	Total / Free Memory: 14.04 MB / 948.00 KB (6.59%)
Basic	
Advanced	
Port Forwarding	
QoS	
Access Restriction	
USB and NAS	
VPN Tunneling	
Administration	
About	

WAN	
MAC Address	00:25:9C:5E:36:03
Connection Type	DHCP
IP Address	207.229.146.105
Subnet Mask	255.255.255.0
Gateway	207.229.146.1
DNS	208.67.222.222:53, 208.67.220.220:53

The next step is to go to **the OpenVPN home page** and download the *OpenVPN Windows Installer OpenVPN* version **2.1.4** . Note that while the latest version is **2.2.0**, there is an error that makes this process much more complicated. The OpenVPN program that we downloaded will allow you to connect to the VPN network, so install it on any computer you want it to be a client. Save *openvpn-2.1.4-install.exe* on your computer.

(#openvpn at irc.freenode.net).

Source Tarball	openvpn-2.2.0.tar.gz	GnuPG
Source Zip	openvpn-2.2.0.zip	GnuPG
Windows Installer	openvpn-2.2.0-install.exe	GnuPG

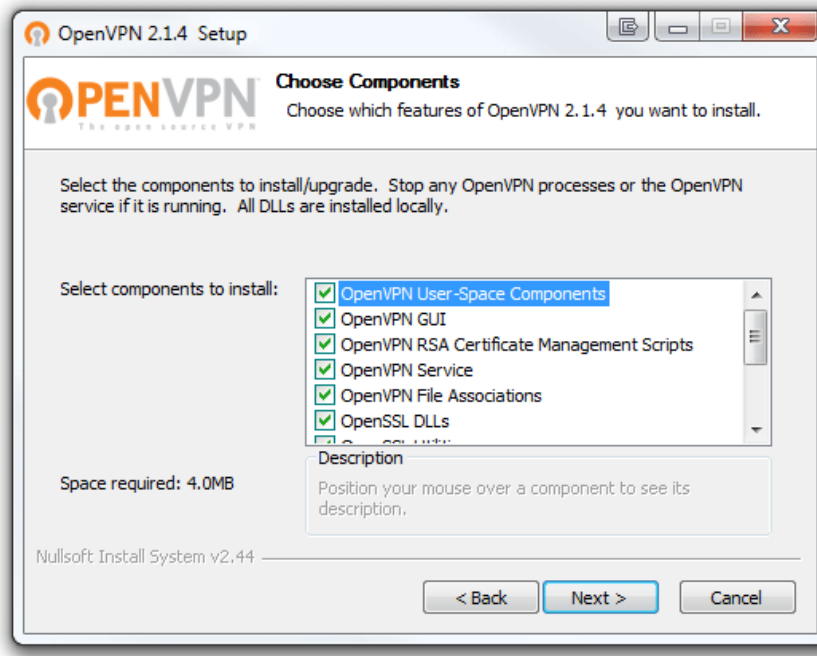
This release is also available as [Debian Lenny](#) and [Ubuntu 10.04](#) packages for the signatures are available [here](#).

OpenVPN 2.1.4 -- released on 2010.11.09 (Change Log)

This is the *old stable release*. Most people should use the *current stable* release.

Source Tarball	openvpn-2.1.4.tar.gz	GnuPG
Source Zip	openvpn-2.1.4.zip	GnuPG
Windows Installer	openvpn-2.1.4-install.exe	GnuPG

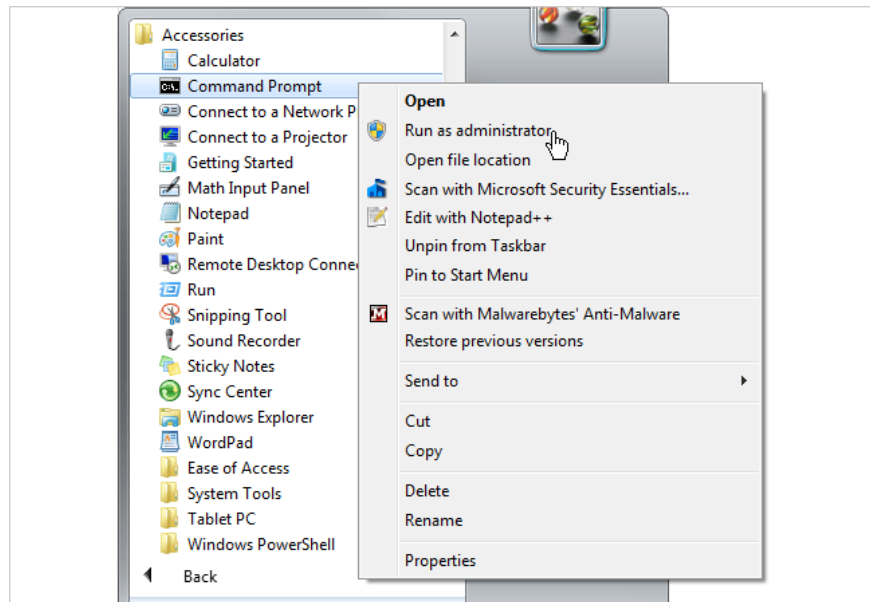
Navigating to the OpenVPN file just downloaded and double-clicking on it, the installation process will begin. The installation is very simple, just keep the default options and click **Next** . During installation, a small pop-up dialog box will appear and ask if you want to install a new virtual private network adapter named **TAP-Win32** , click **Install** .



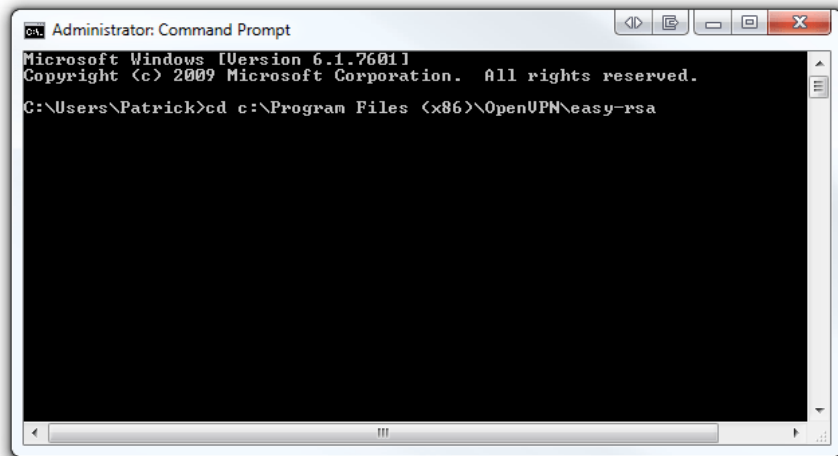
After installation is complete, you start creating Certificates and Keys for device authentication.

Create Certificates and Key

Go to the **Start** menu, select **Accessories** . Right-click *Command Prompt* select *Run as administrator* .

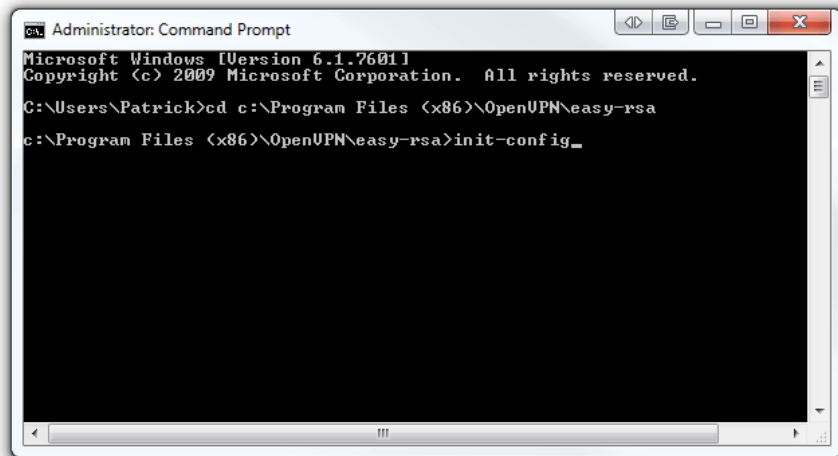


At the command prompt, type `cd c: Program Files (x86) OpenVPNeasy-rsa` if you are running Windows 7 64-bit as shown below. (If using 32-bit Windows 7, type `cd c: Program FilesOpenVPNeasy-rsa`). Press **Enter** .



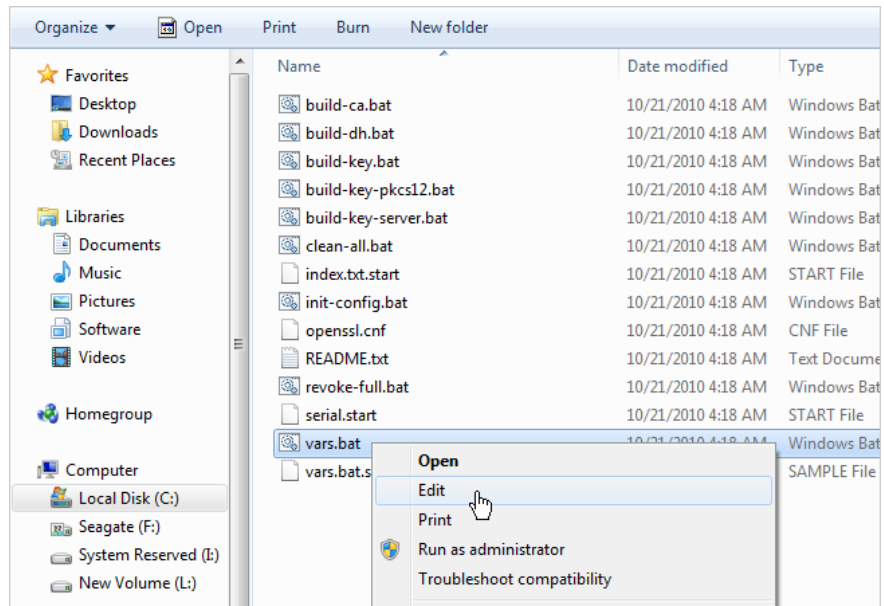
```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Patrick>cd c:\Program Files (x86)\OpenVPN\easy-rsa
```

Now type **init-config** , press **Enter** to copy the two files named *vars.bat* and *openssl.cnf* into the *easy-rsa* folder. Maintaining the command prompt window always opens and switches to the next step.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Patrick>cd c:\Program Files (x86)\OpenVPN\easy-rsa
c:\Program Files (x86)\OpenVPN\easy-rsa>init-config_
```

Open the folder *C: Program Files (x86) OpenVPN\easy-rsa* (or *C: Program Files\OpenVPN\easy-rsa* with 32-bit Windows 7) right-click the **vars.bat** file> select **Edit** to open it in Notepad. However we recommend using *Notepad ++* as a text editor in a much better file. You can download Notepad ++ [here](#) .



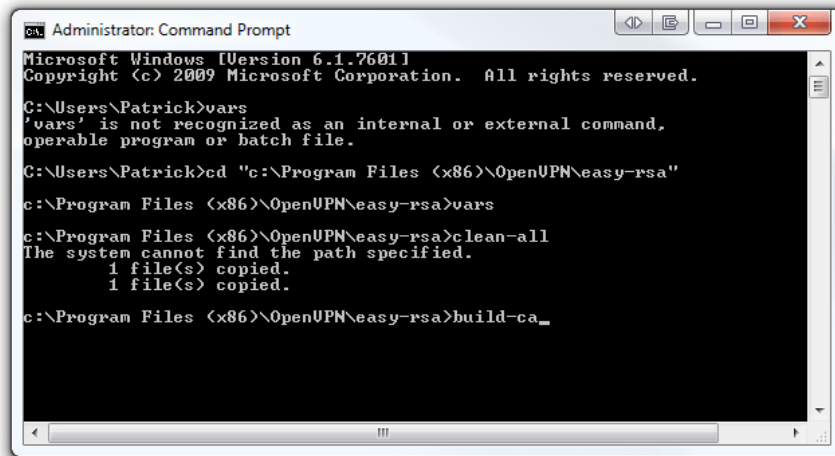
We will be most concerned about the end of this file. Start from line **31** , change the value of *Key_COUNTRY* , *Key_PROVINCE* . to your information. Such as the illustration below:

```

1  @echo off
2  rem Edit this variable to point to
3  rem the openssl.cnf file included
4  rem with easy-rsa.
5
6  set HOME=%ProgramFiles (x86)%\OpenVPN\easy-rsa
7  set KEY_CONFIG=openssl.cnf
8
9  rem Edit this variable to point to
10 rem your soon-to-be-created key
11 rem directory.
12 rem
13 rem WARNING: clean-all will do
14 rem a rm -rf on this directory
15 rem so make sure you define
16 rem it correctly!
17 set KEY_DIR=keys
18
19 rem Increase this to 2048 if you
20 rem are paranoid. This will slow
21 rem down TLS negotiation performance
22 rem as well as the one-time DH parms
23 rem generation process.
24 set KEY_SIZE=1024
25
26 rem These are the default values for fields
27 rem which will be placed in the certificate.
28 rem Change these to reflect your site.
29 rem Don't leave any of these parms blank.
30
31 set KEY_COUNTRY=US
32 set KEY_PROVINCE=IL
33 set KEY_CITY=Chicago
34 set KEY_ORG=HowToGeek
35 set KEY_EMAIL=patrick@howtogeek.com

```

Go back to the command prompt window, type **vars** and press **Enter** , then type **clean-all** , press **Enter** . Finally type **build-ca > Enter** .



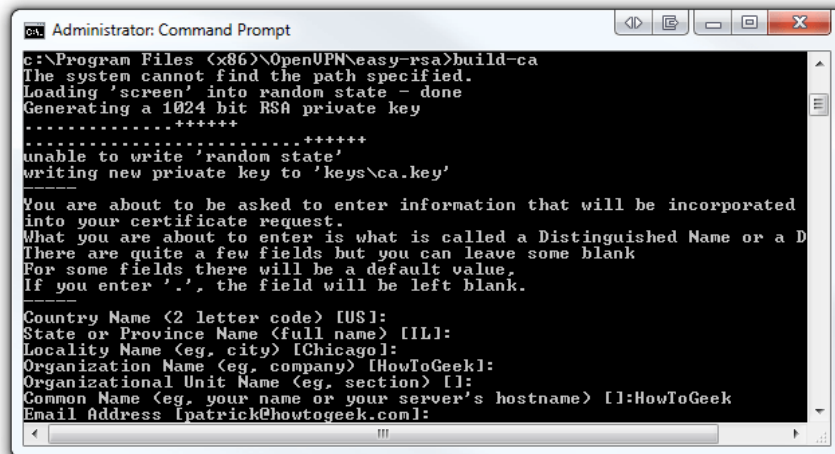
```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Patrick>vars
'vars' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Patrick>cd "c:\Program Files (x86)\OpenUPN\easy-rsa"
c:\Program Files (x86)\OpenUPN\easy-rsa>vars
c:\Program Files (x86)\OpenUPN\easy-rsa>clean-all
The system cannot find the path specified.
1 file(s) copied.
1 file(s) copied.

c:\Program Files (x86)\OpenUPN\easy-rsa>build-ca_
```

After executing the **build-ca** command, you will receive a request to enter information such as *Country* , *State* , or *Locality* . but since we have set up the *vars.bat* file above, just press **Enter**. to forgive. But before that, remember to enter the information in the **Common Name** section like your name. This command will output two files (*Root CA Certificate* and *Root CA Key*) in the *easy-rsa / Keys* folder.



```
Administrator: Command Prompt
c:\Program Files (x86)\OpenUPN\easy-rsa>build-ca
The system cannot find the path specified.
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
unable to write 'random state'
writing new private key to 'keys\ca.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [IL]:
Locality Name (eg, city) [Chicago]:
Organization Name (eg, company) [HowToGeek]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:HowToGeek
Email Address [patrick@howtogeek.com]:
```

Now we will build a Key on the client machine. In the open command prompt, type **build-Key client1** . You can change *client1* to any name you want, just make sure the name matches the *Common Name* when requested. Other parameters are the default, then type 'y' and press **Enter** .

If you get an error ' *unable to write* ' *random state* 'you don't need to worry because your certificates are still working normally. This command will export two files (*Client1 Key* and *Client1 Certificate*) in the *easy-rsa / Keys* folder. If you want to create another Key for any client, repeat the steps above and just make sure to change the *Common Name*.

```
Administrator: Command Prompt
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'IL'
localityName      :PRINTABLE:'Chicago'
organizationName  :PRINTABLE:'HowToGeek'
commonName        :PRINTABLE:'client1'
emailAddress      :IA5STRING:'patrick@howtogeek.com'
Certificate is to be certified until May  4 22:29:30 2021 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
unable to write 'random state'
```

The final certificate is the **Key server** . In the command prompt, type **build-Key-server server** . You can replace 'server' at the end of the command with the name you want (Example: *QTM-Server*) provided that the name must match the information recorded in Common Name. Finally press 'y' to finish. This command will create two files (*Server Key* and *Server Certificate*) in the *easy-rsa / Keys* folder.

```
Administrator: Command Prompt
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'IL'
localityName      :PRINTABLE:'Chicago'
organizationName  :PRINTABLE:'HowToGeek'
commonName        :PRINTABLE:'server'
emailAddress      :IA5STRING:'patrick@howtogeek.com'
Certificate is to be certified until May  4 22:45:25 2021 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
unable to write 'random state'
```

Next we have to create **Diffie Hellman** parameters. The Diffie Hellman protocol allows two users to exchange a secret key on an insecure environment. You can find out more about Diffie Hellman at RSA's website.

In the command prompt, type **build-dh** . This command will export **dh1024.pem** file in *easy-rsa / Keys* folder.

Right-click it and open it with Notepad or Notepad ++, you will see the content as shown below:

```
1 #####
2 # Sample client-side OpenVPN 2.0 config file #
3 # for connecting to multi-client server. #
4 # #
5 # This configuration can be used by multiple #
6 # clients, however each client should have #
7 # its own cert and key files. #
8 # #
9 # On Windows, you might want to rename this #
10 # file so it has a .ovpn extension #
11 #####
12
13 # Specify that we are a client and that we
14 # will be pulling certain config file directive
15 # from the server.
16 client
17
18 # Use the same setting as you are using on
19 # the server.
20 # On most systems, the VPN will not function
21 # unless you partially or fully disable
22 # the firewall for the TUN/TAP interface.
23 ;dev tap
24 dev tun
25
26 # Windows needs the TAP-Win32 adapter name
27 # from the Network Connections panel
28 # if you have more than one. On XP SP2,
29 # you may need to disable the firewall
30 # for the TAP adapter.
31 ;dev-node MyTap
32
33 # Are we connecting to a TCP or
34 # UDP server? Use the same setting as
35 # on the server.
```

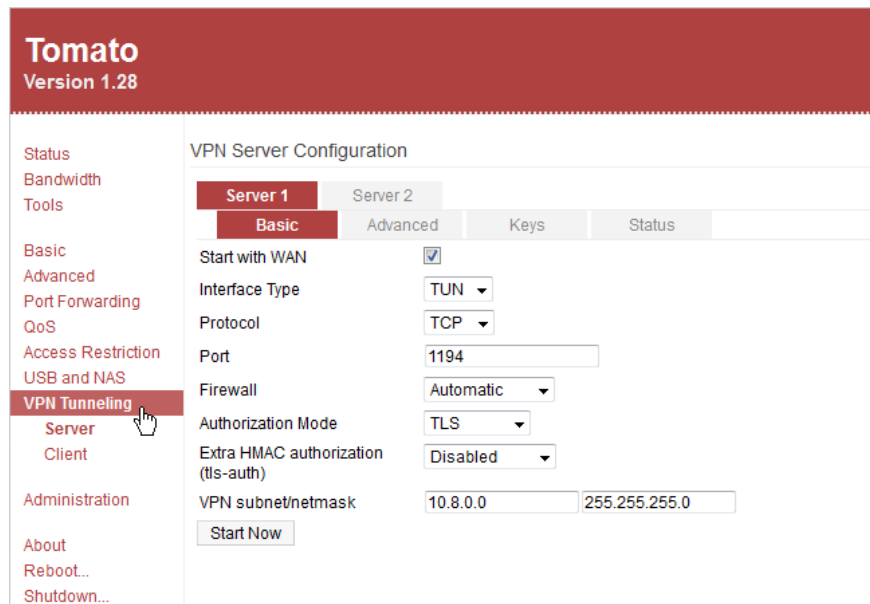
However, we want the *client.ovpn* file to be exported to be similar to the image below. Make sure you have changed DynDNS hostname in line **4** (or change the IP address if it is static). Keep port **1194** intact because this is the standard port of OpenVPN. Next, change lines **11** and **12** by the name of the *Certificate* file and *Key* you created for the client. Save this file as a new *.ovpn* file in the *OpenVPN/config* folder.

```
1 client
2 dev tun
3 proto tcp
4 remote howtogeek.dyndns.org 1194
5 resolv-retry infinite
6 nobind
7 persist-key
8 persist-tun
9
10 ca ca.crt
11 cert client1.crt
12 key client1.key
13 ns-cert-type server
14 cipher AES-128-CBC
15 comp-lzo
16 verb 4
```

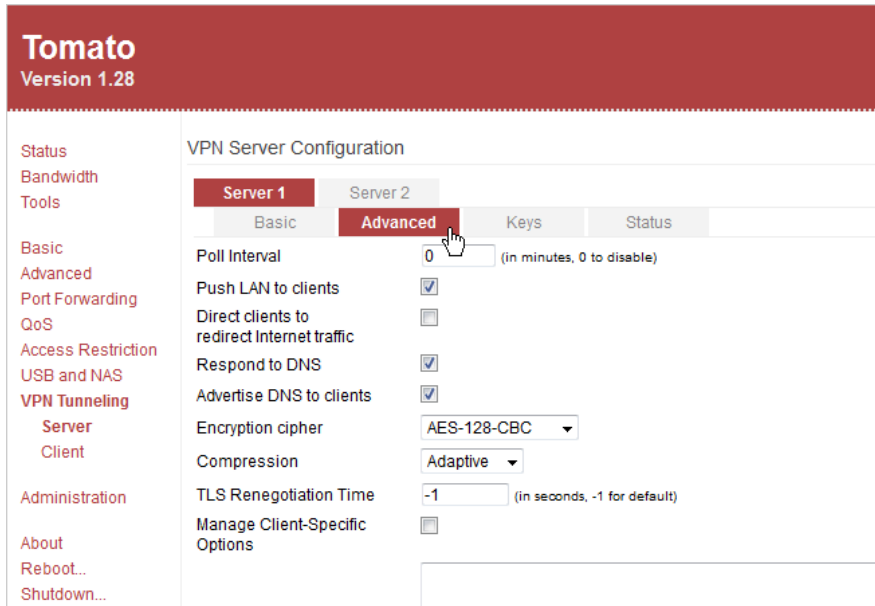
Configuring VPN Tunneling for Tomato

Now we will copy server certificates and keys and paste them into the Tomato VPN menu. We will then test some settings in Tomato, testing the VPN connection.

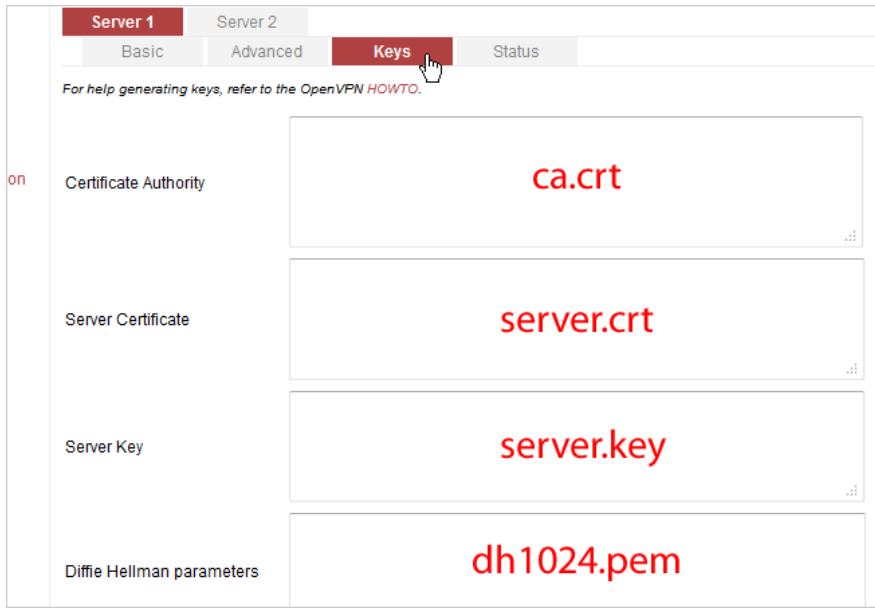
Open the browser and navigate to the router. Click the **VPN Tunneling** menu. Make sure **Server1** and **Basic** are both selected. Set up exactly the following, then click **Save** .



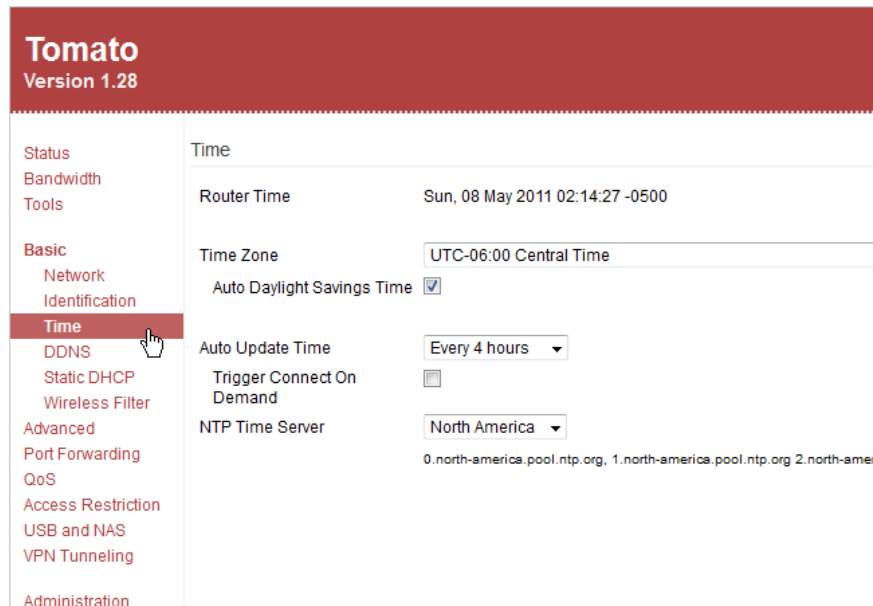
Switch to the **Advanced** tab next to the Basic tab. Set up the image below and click **Save** .



Finally, paste the Key and Certificates we created earlier. Switch to the **Keys** tab next to Advanced. In Windows Explorer, go to *C: Program Files (x86) OpenVPNeasy-rsaKeys* (Windows 7 64-bit) or *C: Program FilesOpenVPNeasy-rsaKeys* on Windows 7 32-bit. Open each corresponding file below (*ca.crt*, *server.crt*, *server.key*, and *dh1024.pem*) with Notepad or Notepad ++ utility and copy the contents. Paste this content into the corresponding boxes. Note that you only need to paste things below --BEGIN CERTIFICATE-- in *server.crt* . OpenVPN will still work properly if you paste the entire content, but it's best to just paste the ' clean ' information into it. Click **Save** and click **Start Now** .



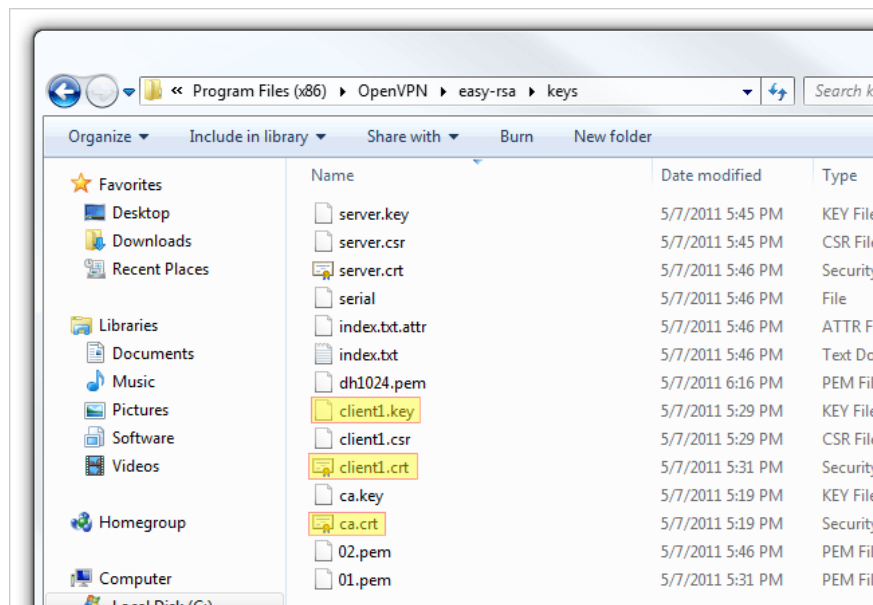
Before we test the VPN connection, there's another problem to check in Tomato. Go to **Basic > Time** menu. It is important to make sure that **Time Router** and **Time Zone display times** are correct with your current time zone. Set the **NTP Time Server section** according to the country you live in.



Set up OpenVPN Client

In this example we use a laptop running Windows 7 as a client. First, you also install OpenVPN for the client as shown above in configuring OpenVPN. Then open *C: Program FilesOpenVPNconfig* , this is where you will paste the files.

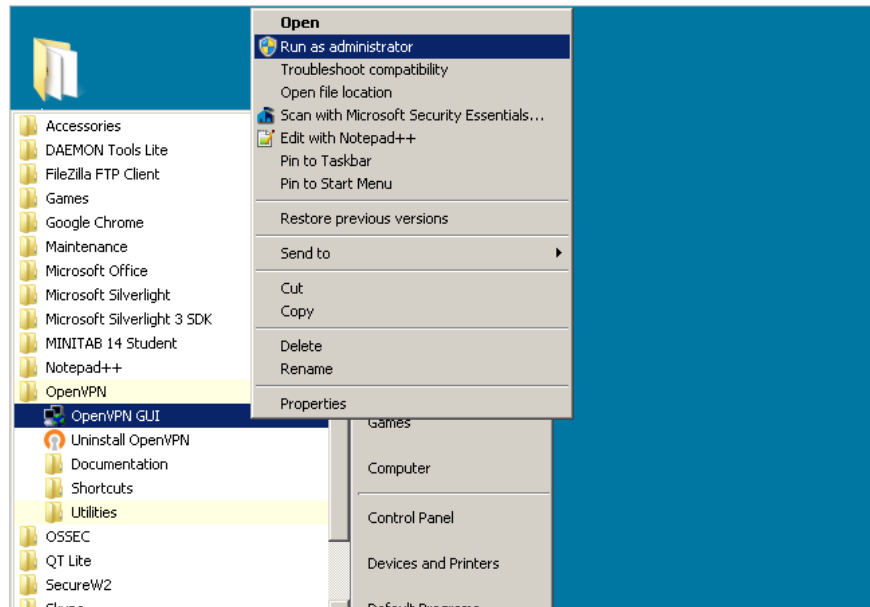
Now go back to the first computer to copy a total of 4 files to the laptop client. Navigate to *C: Program Files (x86) OpenVPNeasy-rsaKeys* and copy the *ca.crt*, *client1.crt* files, and *client1.key* then paste into the client's *config* folder.



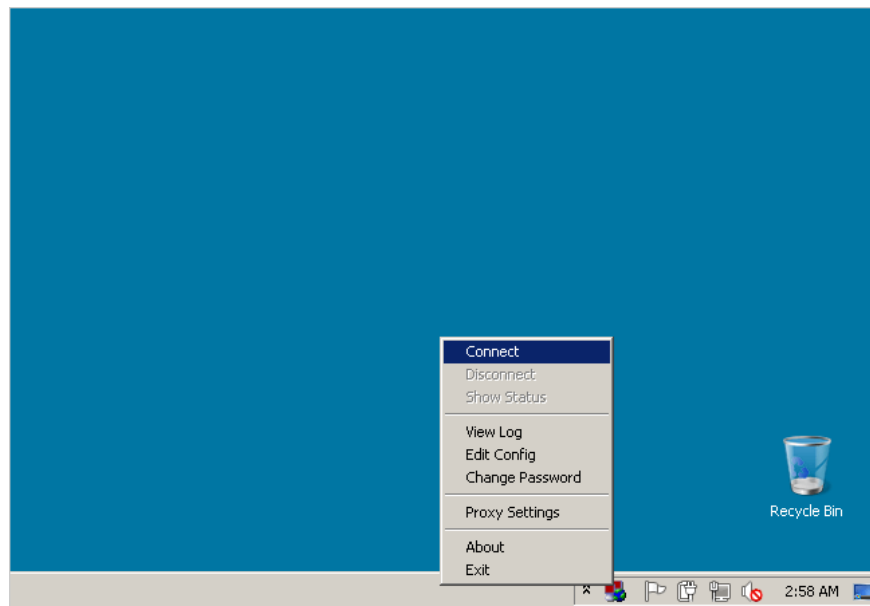
Finally we need to copy a file. Navigate to *C: Program Files (x86) OpenVPNconfig* and copy the previously created *client.ovpn* file, then paste it into the *config* folder.

Test OpenVPN Client

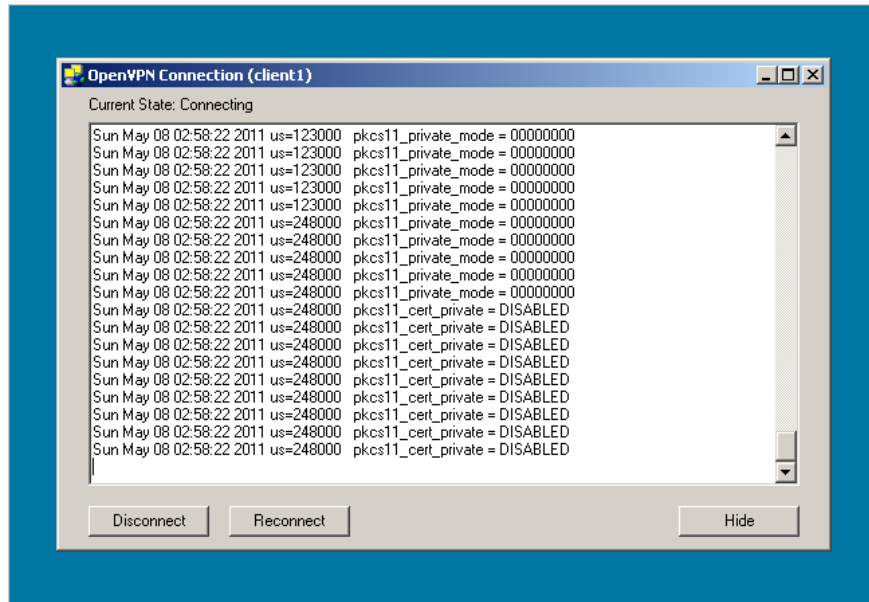
On the laptop client, click the **Windows Start** button > **All Programs** > **OpenVPN** . Right click on the **OpenVPN GUI** file > select **Run as administrator** . Note that you must always run OpenVPN as an *administrator* so it works best. To do this, set it up forever as an administrator by right-clicking on the file, selecting **Properties** , under the **Compatibility** tab, tick the entry ' *Run this program as an administrator* ' .



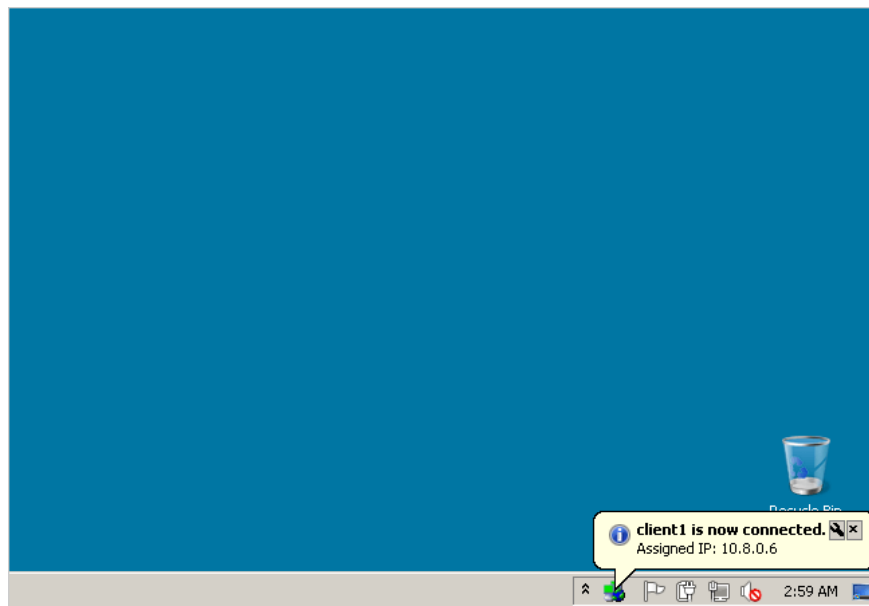
The OpenVPN GUI icon will appear next to the system clock of the taskbar. Right-click this icon and select **Connect** .



A pop-up dialog box will display connection logs.



Once you have connected to the VPN, the OpenVPN icon in the taskbar will turn green and display your virtual IP address.



So you succeeded. You now have a secure connection between the server and the client using OpenVPN and TomatoUSB. To continue checking the connection, try opening a browser on the client and navigating to the Tomato router on the server's network.

You finished reading the article "**Connect anywhere with OpenVPN and Tomato**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.