

# Linux:OpenVPN:ConfigureWebmin

## Contents

- 1 How to configure OpenVPN through Webmin
  - ◆ 1.1 Installing the Webmin module
  - ◆ 1.2 Configuring some basic settings
    - ◇ 1.2.1 Generating a CA certificate
    - ◇ 1.2.2 Generating the server key
    - ◇ 1.2.3 Creating the VPN server
    - ◇ 1.2.4 Generating Client keys
    - ◇ 1.2.5 Enable access for a Client Key
    - ◇ 1.2.6 Exporting the Configuration
  - ◆ 1.3 Connecting a Client
  - ◆ 1.4 Some Notes

## How to configure OpenVPN through Webmin

### Installing the Webmin module

First of all we will need to install the module, without it we will not do very much.

```
# wget http://www.openit.it/downloads/OpenVPNadmin/openvpn-2.5.wbm.gz
```

When logged in to Webmin (Use the MSC theme, so my buttons may look different) go to **Webmin Configuration**



In this new page click on **Webmin Modules**



Now click on **From local file** and select the Local file, afterwards click **Install Module**

**Install Module**

**Install from**

☒ **From local file**  
☐ **From uploaded file**  
☐ **From ftp or http URL**  
☐ **Standard module from www.webmin.com**  
☐ **Third party module from**

...

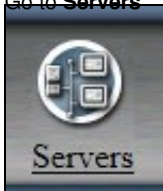
**Ignore dependencies?** ☐ Yes ☒ No

**Grant access to** ☒ Grant access only to users and groups :   
☐ Grant access to all Webmin users

Now wait for Webmin to finish and your module is installed.

## Configuring some basic settings

Go to **Servers**





In the new overview click on **OpenVPN + CA**



Now you should see this:

### OpenVPN Administration

[Certification Authority List](#)

[VPN List](#)

#### New Certification Authority

Name of Certification Authority	changeme
Complete path to openssl.cnf	/etc/openvpn/openvpn-ssl.cnf
Keys directory	/etc/openvpn/keys
Key size (bit)	2048 ▾
Expiration time of Certification Authority key (days)	3650
State	US
Province	NY
City	New York
Organization	My Org
Email	me@my.org

Save

Start OpenVPN

Start OpenVPN activating all configurations present in OpenVPN home with e

First let's continue the set up of the module. Click on **Moduel Config**. Here you will need to update the **Command to start Bridge**, **Command to stop Bridge** and **Path to DOWN-ROOT-PLUGIN**. You can find them with the following commands in a shell:

```
# locate bridge_start
# locate bridge_end
# locate openvpn-down-root
```

Now click **Save**.

## Generating a CA certificate

First of all we will need a CA to sign and revoke our other certificates. So click on **Certification Authority List**. No CA's should be listed. Time to create one.

To create one fill out the form:

Field name	What to fill in
Name of Certification Authority	This should be either a domain name or your full name
Complete path to openssl.cnf	Leave this unchanged, Webmin is usually correct
Keys directory	You cannot and should not change this
Key size (bit)	The best is to leave it at 2048 bit, if you increase it make sure you have a strong server since then it could take a while
Expiration Time of Certification Authority key (days)	This is 10 years by default, which is generally a good way to go
State	Your state
Province	Your province
City	Your city
Organization	Your organization
Email	Your e-mail address

Then click **Save**. When the long process of about 2 hours is done. Go back to the CA list, you should see your CA in the list.

## Generating the server key

Click on **Keys list**.

The first thing you should do now is create a server key, we will need to this to start/create a vpn server. Once again fill in the form. A large portion is copied from the CA and should be correct:

Field name	What to fill in
Key name	I usually put the server name here
Key password	Leave empty for the Server key
Key Server	Select server

Now click **Save**.

## Creating the VPN server

Go back to the index of the **OpenVPN + CA**. Here click on **VPN List**.

OpenVPN Administration

VPN server list:

ca (Certification Authority): test.ca ▼

New VPN server

Creation of new VPN Server: sel

VPN server list with simmetric key

VPN List is empty

New VPN Server with symmetrical key

Creati

Now for the scary stuff. Make sure the CA that is selected is the one we just generated and click on **New VPN Server**. The part we are going to do now is very tricky. I will try to explain it as good as I can, however some networking knowledge is required.

Field Name	What to fill in
Name	This may be any name, however try to make it descriptive
Port	Default is 1194, it is a good port to use
Proto	I use tcp-server here, because I find it easier to connect to from foreign networks
Device	<p>You have 2 options here: <i>tun</i> and <i>tap</i>:</p> <p><b>tun:</b> Tun is short for tunnel, this device will simply create a complete new device and LAN segment for your clients. You will need full-blown routing if you want to enable access to others LANs from this VPN Segment. However it is good to create an isolated VPN Segment.</p> <p><b>tap:</b> Tap is used when you want to bridge the VPN adapter onto a real interface on your server, this way you will make your server hand out internal IPs in your local-scope. This creates the same idea as the old PPTP VPNs in windows servers, but more secure.</p> <p>I choose tap, since I want people to become part of my local-lan and want minimum routing to be set up.</p>
Bridge Device	I usually fill in br0, this is only required when using tap
Network Device for Bridge	Usually this will be eth0. This is the device that will be linked to the Tap adapter. Always use your local-lan NIC if you want people to become part of your local-lan.
IP config for bridge	Fill in the current IP of the interface that is going to be bridged, and the current netmask
IP-Range for Bridge-Clients management	I recommend using a scope outside your normal DHCP Scope, but in your subnet
Choose key	I always select yes here, and as port I usually take something like 10001 or up
Enable TLS and assume server role during TLS handshake	Select your server key
option client-to-client	Set this to yes for more security
option duplicate-cn	Set to yes
option tls-auth	This will allow multiple clients to connect to the server with the same certificate. I usually select no, but if you want to avoid generating keys for every user set this to yes.
option cipher	Set this to yes
up (script execute after VPN up)	To support windows clients set this to <i>BF-CBC 128 bit default key (variable)</i>
Now click <b>Save</b> .	Use this to re-add your default gateway: <i>route add default gw &lt;gateway ip&gt;</i>

If everything was filled out correctly you should see a new VPN server in the list. Now click **Start** and pray that the server does not lose its connectivity. If it does you have filled in an invalid IP somewhere, probably the gateway. If it starts and the server stays connected, you have set up your first SSL VPN using OpenVPN.

### Generating Client keys

Go back to the main module screen for the **OpenVPN + CA**. Click on **Certification Authority List**. Go to **Keys list**.

Now fill out the form as follows:

Field name	What to fill in
Key name	I usually use the name to whom I am going to give this key
Key password	Fill in a password of minimal 4 characters, this is needed upon connecting to use the key
The rest should be fine by default. Now click <b>Save</b> .	

### Enable access for a Client Key

From the index click on **VPN list**. Now select the **Client List** link that belongs to your server. Click on **New VPN Client** and fill in the form:

Field name	What to fill in
Name	Select the certificate to link to the server here
remote	Fill in the IP that clients will use to connect to, usually your public IP
Additional Configuration	I use this to push the route for my network so I add e.g.: <i>route 192.168.0.0 255.255.255.0</i> . You will need to add your own network here of course
Now click <b>Save</b> .	

### Exporting the Configuration

Back in the **Client list** Click on the **Export** link. This will download a .tgz file. This file can be sent/given to the user.

### Connecting a Client

First download the [Windows OpenVPN Client](#)

Install it, and please for the love of god do not refuse the driver (If you do you will not be able to fix this). Unpack the .tgz file into the **configs** directory of the OpenVPN install directory. Now start the OpenVPN GUI (**NOTE:** For Vista and up *Run as Administrator*). You should be able to connect. When clicking on connect you will be asked for a password, this is the password you used when creating the key.

### Some Notes

Be patient, setting up an OpenVPN server can take a lot of time and practice. And can be frustrating at times. But if you are persistent you will succeed eventually.

I hope this HowTo will help you get started.

---

Back to [Linux:KnowledgeBase](#)

[Download this article as a PDF](#)