Your libre router and you!

Dear Customer,

Thank you for purchasing one of the first freedom respecting routers on the market. This router runs the libreCMC GNU/Linux distro : a collection of *free software* that respects your freed+om. With the software on this router being *free software*, you have the freedom to review what the software on the router is doing, make changes to the software, re-flash the router with your modified copy and share the changes that you make. By choosing this router, you the customer, will help pave the way for more freedom respecting hardware in the future.

Setup for those who are not connecting to a VPN:

0) Plug ethernet cable from Cable Modem / DSL Modem to the WAN port (labeled WAN).

1) Connect an ethernet cable from your computers LAN port to the LAN port on the mini router (labeled LAN).

2) Connect the power cable in for the mini router

(will see green lights on the front if it successfully boots)

3) If connecting to the default wireless network rather than by ethernet cable use the following settings:

wireless network name: libreCMC
password: librecmc

4) To administer your router, go to : https://192.168.10.1

You may encounter a warning such as "Warning: Potential Security Risk Ahead" or "Your connection is not private". Despite the scary sounding warning this is the result of a self-signed certificate and your connection is slightly more secure than it would be otherwise. Click the Advanced button and then "Proceed to 192.168.10.1 (unsafe)" or "Accept the Risk and Continue" depending on your browser.

Setting a password for your Wireless Network (highly recommended)

1. To change wifi password, enter https://192.168.10.1 into a web browser of a computer attached to the network, login.

2. Then go to : Network -> Wireless.

3. Click the "edit" button on the right side of "libreCMC".

4. Click the "Wireless Security" tab.

5. Enter a new password in the "Key" text box.

6. Then click "Save & Apply" at the bottom of the page.

Browse the web and enjoy! If all of your machines use "DHCP" for their network, everything should just work. Please refer to your modem 's user guide or the libreCMC wiki for help.

Product Information and Support

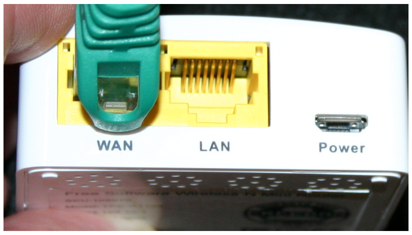
For additional documentation and support visit us on the web: https://www.thinkpenguin.com/support

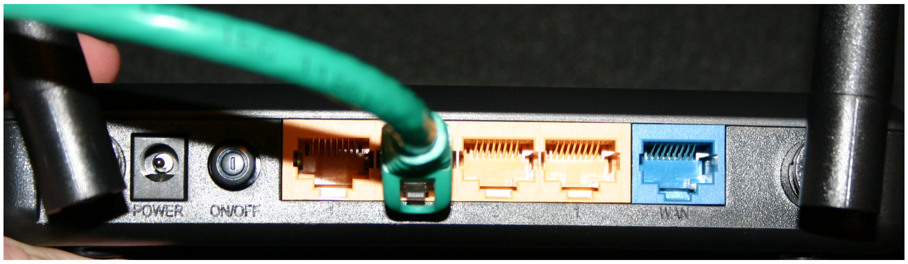
Free Software Wireless-N Mini Router v2
SKU: 107410
Model: TPE-R1200

Free Software Wireless-N Mini Router
SKU: 106970
Model: TPE-R1100

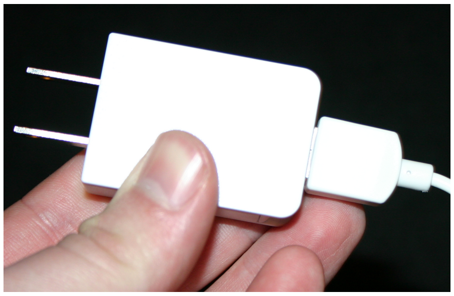
Setup instructions for those who purchased VPN service with the router:

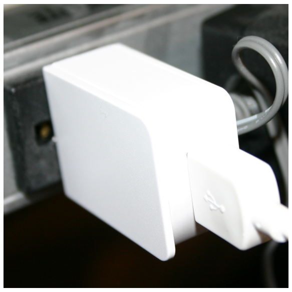
1. Connect an Ethernet cable from the WAN port on the Mini Router (left) to a LAN port on your modem or primary router (right).



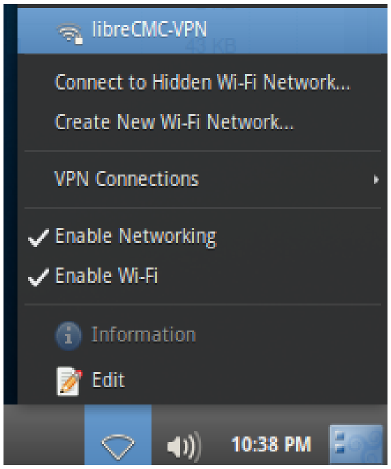


2. Connect the USB cord to the Mini Router where it says Power (left), connect the USB cord at the other end to the power adapter (center), and the power adapter to a wall outlet (right).



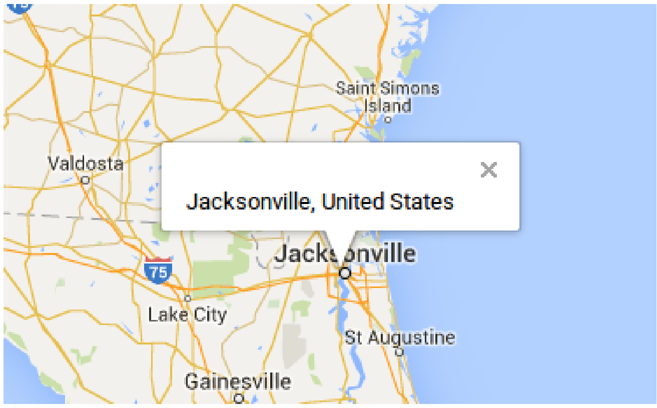


3. Connect your computer / wireless devices to the libreCMC-VPN network (default password: librecmc) whenever you want to surf psudo-anonymously.



Things to note: A VPN connection may result in problems with some online web sites that depend on correct location data to operate. This is primarily true for stores, banks, and commercial video streaming sites. If you encounter a problem with a site you may find an account temporarily locked or an order cancelled. This is because traditional electronic payment systems don't have an effective means of stopping fraud making any payments via Visa/Master Card/PayPal/etc risky. As such merchants refuse business to anonymous individuals to reduce risk when users pay with these mechanisms. Fortunately there is a solution. Cryptocurrencies are quickly becoming the online equivalent of cash. Not controlled by governments, banks, or other entities they act as a safer lower cost solution to payment acceptance.

4. Open your web browser and check the IP address and location that your computer appears to be coming from. One such site you can utilize for this purpose is www.infosniper.net



If your in New Hampshire and the site indicates your browsing from Jacksonville, Florida for instance then your connection is now psudo-anonymous.

Please note that the level anonymity should be adequate for the majority, but may not be sufficient to protect against more sophisticated adversaries targeting groups such as journalists, whistleblowers, dissidents, etc.

Note: We have changed the default Mini Router IP to maximize out-of-the-box compatibility: 192.168.3.1
To change the Mini Router's SSID password open your browser, login to https://192.168.3.1 (default password 'none'), Network -> Wireless, click edit next to libreCMC-VPN, click Wireless Security, enter a new password in the Key box, and click Save & Apply.

Mullvad VPN Setup Instructions

(this is applicable to users who did not purchase VPN service with router, for generic instruction with other VPN providers see README on CD)

1. Log into Mullvad with your account number.
2. Go to the Download page and select Generate OpenVPN configuration file for OpenVPN (under where it says other VPN software).
3. Select Linux for the platform, Sweeden for the Location, and TCP 443 for the port (we are really just getting the ca file here)
4. Click the Download button and extract the Mullvad_ca.crt file that is found in the root of the downloaded ZIP file to a directory on your computer.
5. Connect a network cable from the computers LAN port to the LAN port on the router
6. Open a browser and go to https://192.168.10.1 (you will see a scary warning message about security, you need to add an exception, you may need to click an advanced link to do this)
7. Login and set a password (there is no password set by default so just hit the login button)
8. Click the Go to password configuration link and set a password
9. Click Save & Apply button at the bottom of the page once entering a login password for the router
10. On the same page, in the SSH Access section, set the interface to LAN. Click the Save & Apply button.
11. As your upstream router may be in conflict with your ThinkPenguin router set a different IP addresses

Click the Edit button under Network > Interface > LAN to change your routers IP to 192.168.8.1 (enter 192.168.8.1 under where it says IPv4 address)

12. Click Save & Apply button at bottom of page
13. Enter https://192.168.8.1/ into your browser (you will need to add a security exception again, ie firefox click Advanced button and Accept the Risk and Continue button)
14. Login using your new password
15. Connect an ethernet cable from the WAN port on your router to an upstream modem or router
16. Navigate to System > Software and press Update lists button
17. In download and install package text box enter:

```
openvpn-openssl
luci-app-openvpn
openssl-util
```

18. Open a browser and navigate to http://192.168.8.1/ (the routers IP)
19. From the menu go to Services > OpenVPN
20. In the text field at the bottom, enter “mullvad_client” as a new name
21. Select “Simple client configuration for a routed point-to-point VPN” and click the Add button.
22. You will immediately be taken to the configuration page. Click on “Switch to advanced configuration.”
23. Click the “Networking” link at the top of the page
24. Delete anything in the ifconfig field
25. Make sure the dev text field has "tun" in it (without the quotes)
26. Make sure the port text field has "1194" in it (if it does not exist select port from the drop down list at the bottom and click Add button)
27. Make sure the box is checked for the nobind field
28. Click the Save button at the bottom of the page
29. Click on the “VPN” link at the top of the page
30. Make sure the Client field is set to checked (if it does not exist select client from the additional field down down menu and click Add to add it)
31. Set the auth_user_pass field to “/etc/openvpn/userpass.txt” (without the quotes, if it does not exist select auth_user_pass from the additional field drop down menu and click Add to add it)
32. Set the remote field to se.mullvad.net (you can set this to whatever server you want: http://www.mullvad.net/servers, if the field does not exist select remote from the additional field drop down menu and click Add to add it)
33. Click the Save button at the bottom of the page
34. Now click on the "Cryptography" link
35. In the ca field upload the Mullvad_ca.crt file that you downloaded earlier (if the field does not exist select ca from the additional field drop down menu and click Add to add it)
36. Click the Save button at the bottom
37. From the menu at the top, select Network > Interfaces
38. Click the “Add new interface” button
39. Name of new interface: enter “MULLVAD_VPN” (this must be entered exactly as shown)
40. Set the Protocol of the new interface field to Unmanaged
41. Under Cover the following interface select Custom Interface and enter tun0 into the field and hit enter
42. Click Save & Apply
43. Open a terminal and enter "ssh -l root 192.168.8.1" (without the quotes)

Directions continue onto the next page

44. Enter yes and hit enter to accept the warning about the authenticity not able to be established
45. Enter your router login password
46. Enter "cat > /etc/openvpn/userpass.txt << EOF" without the quotes and hit enter
47. Enter your mullvad VPN account number and hit enter (DO NOT enter any spaces that are in the account number)
48. Enter "M" without the quotes and hit enter
49. Enter "EOF" without the quotes and hit enter
50. Enter "chmod 0400 /etc/openvpn/userpass.txt" without the quotes and hit enter to set the proper file permissions
51. Copy and paste the following:

```
cat >> /etc/config/firewall << EOF
config zone
option name 'VPN_FW'
option input 'REJECT'
option output 'ACCEPT'
option forward 'REJECT'
option masq '1'
option mtu_fix '1'
option network 'MULLVAD_VPN'
config forwarding
option dest 'VPN_FW'
option src 'lan'
EOF
```

52. Hit the enter button after copy and pasting the above.
53. Login to your router again from a browser (enter https://192.168.8.1)
54. Navigate to Network > Interfaces > LAN > DHCP Server (found below the “Common Configuration” section) → Advanced Settings.
55. In the “DHCP-Options” field enter the value “6,10.8.0.1,193.138.218.74”
56. Click on Save & Apply
57. Go to System > Scheduled Tasks
58. Copy and paste "*/1 * * * * sed -i '/secret/d' /tmp/etc/openvpn-mullvad_client.conf" (without the quotes) into the scheduled tasks box
59. Click Submit button
60. Navigate to Services > OpenVPN
61. Enable the checkbox beside mullvad_client, and click Save & Apply
62. Click on the Start button found in that same row
63. You might have to give this 1-2 minutes to start (if you hit refresh button in your browser it should eventually say Yes under the started column)
64. Go to System > Startup
65. Click restart button the on cron line (under the initscript column)
66. Go to Network > Firewall
67. Click on the Edit button for the "lan" zone
68. Under Inter-Zone Forwarding and Allow forward to destination zones uncheck the box that says WAN:
69. Click Save & Apply button

Private Internet Access VPN Setup Instructions

(this is applicable to users who did not purchase VPN service with router, for generic instruction with other VPN providers see README on CD)

1. To utilize PIA with our libre router software find your login credentials (probably found in your email or via logging in to the site).
2. Create a folder in your home directory named librecmc-openvpn-setup and copy the Default-VPN-Config.tar.gz file from the included CD to this directory. Extract the files.
3. Create a directory in the etc folder called openvpn.
4.You will need to extract an ovpn config file, the ca.crt file, and the crl.pem file to your newly created etc/openvpn folder. You can get the zip file containing the ovpn, crl.pem, ca.crt files from:
https://www.privateinternetaccess.com/openvpn/openvpn.zip. Note: You can select any of the ovpn files. The file determines the location of the server that your VPN router will pass traffic through.
5. Open a text editor such as gedit and enter your username and password. The user name must go on the first line followed by the password on the next. The user name and password can be found in an email sent by Private Internet Access following sign up. The email is titled “Private Internet Access Account Activated”. Save file as etc/openvpn/key.txt after creating it. Example of the file:

```
p9302930294
JiiF3kWofkF
```

6. Open the etc/config directory and edit the openvpn file in a text editor. Change the following line: option config /etc/openvpn/ to include your opvn file that you downloaded to the etc/openvpn directory in the earlier step. Save file after editing. Example:

```
option config “/etc/openvpn/US New York City.ovpn”
```

7. In the etc/openvpn ovpn file you will also need to change the line that reads auth-user-pass to auth-user-pass key.txt
8. Open the librecmc-openvpn-setup directory and right click on the etc folder. You need to “tar it up”. To do that select the Compress option. Then click the Create button and Close button respectively. Make sure the tar.gz option in the drop down is selected for the type of compression.
9. Connect an ethernet cable from the LAN port of the mini VPN router to the ethernet port on your computer. Plug the mini VPN router in.
10. On your computer disconnect from the wifi (if you are connected to an access point)
11. On your computer open a web browser and enter https://192.168.10.1/ into the address bar. Then hit enter.
12. Accept the security warning and continue anyway
13. Click the Login button (you may need to enter 'root' for the user name and 'none' as the password if your changing providers)
14. Click Go to password configuration... link
15. Enter a password in the Password box and again in the Confirmation box. Take note of the router password as you'll need it to configure the router in the future.
16. Scroll down to the bottom of the page and click the Save and Apply button. Wait a few moments for changes to take affect.
17. Go to System > Backup / Flash Firmware
18. Click Browse button under the Backup / Restore section
19. Select the librecmc-openvpn-setup/etc.tar.gz file you created earlier and click the Upload Archive button. Let the router restart. Then login.
20. Set DNS server in Network > Interfaces > WAN > Advanced Settings and enter a DNS. Uncheck Use DNS servers advertised by peer to do this. Enter 84.200.69.80 in the Use custom DNS servers box. Click save.
21. Set the IP to 192.168.3.1 : Network > Interfaces. Next to LAN click Edit. In the IPv4 address change the address to 192.168.3.1. Click Save. Note: If your primary router is using a 192.168.3.x subnet then you will need to change the mini router's subnet to something else.
22. Network > Wifi and click the Edit button next to where it says the SSID name (libreCMC).
Scroll down to the bottom of the page where it says Interface Configuration. Under the General Setup there is a box that says ESSID next to it. Change the name from libreCMC to libreCMC-VPN. Click the Wireless Security tab and enter a password where it says Key. Take note of this. It is the password you'll need to connect to your libreCMC-VPN access point in the steps below. Click Save & Apply button.
24. Give it 30 seconds and switch your ehternet cable from the LAN port on your computer to a LAN port on your primary router. Then the other end to the WAN port on your mini VPN router.
25. You can now turn the mini VPN router off and on again (pull the power on the router and reconnect). Give the mini VPN router a minute or two to boot up.
26. Turn your wifi back on, and select the libreCMC-VPN network from the list of access points. If you did not enter a password for the SSID as instructed above the default password is librecmc. Otherwise enter the password you selected for the SSID to connect. You should now be able to open a browser and confirm that your connected through the VPN by visiting a geolocation service website. Example http://www.infosniper.net/. It should indicate that your visiting from a city, state, and country of the .ovpn file selected earlier.

IPredator VPN Setup Instructions

(this is applicable to users who did not purchase VPN service with router, for generic instruction with other VPN providers see README on CD)

1. To utilize IPredator VPN with our libre router software find your login credentials (probably found in your email or via logging in to the site).
2. Create a folder in your home directory named librecmc-openvpn-setup and copy the Default-VPN-Config.tar.gz file from the included CD to this directory. Extract the files.
3. Create a directory in the etc folder called openvpn.
4.You will need to download the Command line Ipredator-CLI-Password.conf file from https://ipredator.se/account/dashboard#downloads to the etc/openvpn folder.
5. Open a text editor such as gedit and enter your username and password. The user name must go on the first line followed by the password on the next. The user name and password are that which you selected on sign-up. Save file as etc/openvpn/IPredator.auth after creating it. Example of the file:

```
bobjoe
JiiF3kWofkF
```

6. Open the etc/config directory and edit the openvpn file in a text editor. Change the following line: option config /etc/openvpn/ to include your IPredator-CLI-Password.conf file that you downloaded to the etc/openvpn directory in the earlier step. Save file after editing. Example:

```
option config “/etc/openvpn/IPredator-CLI-Password.conf”
```

7. Open the librecmc-openvpn-setup directory and right click on the etc folder. You need to “tar it up”. To do that select the Compress option. Then click the Create button and Close button respectively. Make sure the tar.gz option in the drop down is selected for the type of compression.
8. Connect an ethernet cable from the LAN port of the mini VPN router to the ethernet port on your computer. Plug the mini VPN router in.
9. On your computer disconnect from the wifi (if you are connected to an access point)
10. On your computer open a web browser and enter https://192.168.10.1/ into the address bar. Then hit enter.
11. Accept the security warning and continue anyway
12. Click the Login button (you may need to enter 'root' for the user name and 'none' as the password if your changing providers)
13. Click Go to password configuration... link
14. Enter a password in the Password box and again in the Confirmation box. Take note of the router password as you'll need it to configure the router in the future.
15. Scroll down to the bottom of the page and click the Save and Apply button. Wait a few moments for changes to take affect.
16. Go to System > Backup / Flash Firmware
17. Click Browse button under the Backup / Restore section
18. Select the librecmc-openvpn-setup/etc.tar.gz file you created earlier and click the Upload Archive button. Let the router restart. Then login.
19. Set DNS server in Network > Interfaces > WAN > Advanced Settings and enter a DNS. Uncheck Use DNS servers advertised by peer to do this. Enter 84.200.69.80 in the Use custom DNS servers box. Click save.
20. Set the IP to 192.168.3.1 : Network > Interfaces. Next to LAN click Edit. In the IPv4 address change the address to 192.168.3.1. Click Save. Note: If your primary router is using a 192.168.3.x subnet then you will need to change the mini router's subnet to something else.
21. Network > Wifi and click the Edit button next to where it says the SSID name (libreCMC).
Scroll down to the bottom of the page where it says Interface Configuration. Under the General Setup there is a box that says ESSID next to it. Change the name from libreCMC to libreCMC-VPN. Click the Wireless Security tab and enter a password where it says Key. Take note of this. It is the password you'll need to connect to your libreCMC-VPN access point in the steps below. Click Save & Apply button.
22. Give it 30 seconds and switch your ehternet cable from the LAN port on your computer to a LAN port on your primary router. Then the other end to the WAN port on your mini VPN router.
23. You can now turn the mini VPN router off and on again (pull the power on the router and reconnect). Give the mini VPN router a minute or two to boot up.
24. Turn your wifi back on, and select the libreCMC-VPN network from the list of access points. If you did not enter a password for the SSID as instructed above the default password is librecmc. Otherwise enter the password you selected for the SSID to connect. You should now be able to open a browser and confirm that your connected through the VPN by visiting a geolocation service website. Example http://www.infosniper.net/. It should indicate that your visiting from another city, state, and/or country.

AirVPN VPN Setup Instructions

(this is applicable to users who did not purchase VPN service with router, for generic instruction with other VPN providers see README on CD)

1. To utilize AirVPN with our libre router software find your login credentials (probably found in your email or via logging in to the site).
2. Create a folder in your home directory named librecmc-openvpn-setup and copy the Default-VPN-Config.tar.gz file from the included CD to this directory. Extract the files.
3. Once you have an account go to https://airvpn.org/generator/ and select the following configuration:
Under "1. Choose your Operating System" Select Linux
Under "2. Choose servers" Pick a server
Under "3. Protocols" Select UDP and then check the 'Advanced mode' box.
On the right you will see a box for 'Separate keys/certs from .ovpn file', check this box
Under 4. "Terms of Service" Check the boxes that say 'I have read and I accept the Terms of Service'
and 'I HEREBY EXPLICITLY ACCEPT POINTS 8, 10, 11'
4. Click the Generate button and click the tar.gz to save the resulting AirVPN.tar.gz file to your librecmc-openvpn-setup/etc/ directory
5. Extract AirVPN.tar.gz to librecmc-openvpn-setup/etc/ and delete the AirVPN.tar.gz file
6. Rename the AirVPN folder that is extracted in prior command to openvpn
7. In the openvpn directory you will need to edit a file that ends in .ovpn
Find the following line: explicit-exit-notify 5 and comment out the line so it looks like this: #explicit-exit-notify 5

Then remove the quotes from the following lines such that it looks like:

```
ca ca.crt
cert user.crt
key user.key
tls-auth ta.key 1
```

8. Save and exit
9. Rename the .ovpn file to have an extension of .conf
10. Edit librecmc-openvpn-setup/etc/config/openvpn
Replace the line that reads:

```
option config /etc/openvpn/
```

With the following (but change AirVPN_Netherlands_UDP-443.conf to that of your .ovpn file that was rename to .conf in step 9):

```
option config /etc/openvpn/AirVPN_Netherlands_UDP-443.conf
```

11. Save and exit
12. Go to your librecmc-openvpn-setup folder and compress the etc folder (make sure to save it as a tar.gz file, and not a .zip file)
13. If you open the etc.tar.gz file you just created you should see a folder in it called etc
14. Open up a web browser and connect the ethernet cable from the lan port on the mini router to your computer (disable wireless on your computer temporarily) and plug the power in; wait about 2 minutes for the router to boot up
15. Open a browser (you may have to use Firefox) and go to https://192.168.10.1/ - you will probably get a warning message such as 'Your connection is not secure'. This is suppose to occur. Nothing is wrong. Click Advanced and Add Exception (in Firefox anyway) so you can continue. You will also need to click Confirm Security Exception (in Firefox). Other browsers will be slightly different.
16. Click Login (there is no password set by default)
17. Click Go to password configuration... link
18. Enter a password and hit save and apply
19. Go to System > Backup / Flash Firmware
20. Click Browse button under the Backup / Restore section
21. Select the librecmc-openvpn-setup/etc.tar.gz file you created earlier and click the Upload Archive button. Let the router restart. Then login.
22. Set DNS server in Network > Interfaces > WAN > Advanced Settings and enter a DNS. Uncheck Use DNS servers advertised by peer to do this. Enter 84.200.69.80 in the Use custom DNS servers box. Click save.
23. Set the IP to 192.168.3.1 : Network > Interfaces. Next to LAN click Edit. In the IPv4 address change the address to 192.168.3.1. Click Save. Note: If your primary router is using a 192.168.3.x subnet then you will need to change the mini router's subnet to something else.
24. Network > Wifi and click the Edit button next to where it says the SSID name (libreCMC).
Scroll down to the bottom of the page where it says Interface Configuration. Under the General Setup there is a box that says ESSID next to it. Change the name from libreCMC to libreCMC-VPN. Click the Wireless Security tab and enter a password where it says Key. Take note of this. It is the password you'll need to connect to your libreCMC-VPN access point in the steps below. Click Save & Apply button.
25. Give it 30 seconds and switch your ehternet cable from the LAN port on your computer to a LAN port on your primary router. Then the other end to the WAN port on your mini VPN router.
26. You can now turn the mini VPN router off and on again (pull the power on the router and reconnect). Give the mini VPN router a minute or two to boot up.
27. Turn your wifi back on (on your computer), and select the libreCMC-VPN network from the list of access points. If you did not enter a password for the SSID as instructed above the default password is librecmc. Otherwise enter the password you selected for the SSID to connect. You should now be able to open a browser and confirm that your connected through the VPN by visiting a geolocation service website. Example http://www.infosniper.net/. It should indicate that your visiting from another city, state, and/or country.

NordVPN Setup Instructions

(this is applicable to users who did not purchase VPN service with router, for generic instruction with other VPN providers see README on CD)

1. To utilize NordVPN with our libre router software find your login credentials (probably found in your email or via logging in to the site).
2. Create a folder in your home directory named librecmc-openvpn-setup and copy the Default-VPN-Config.tar.gz file from the included CD to this directory. Extract the files.
3. Create a directory in the etc folder called openvpn.
4.You will need to extract an ovpn config file to your newly created etc/openvpn folder. You can get the zip file containing the ovpn file from: https://nordvpn.com/api/files/zip. Note: You can select any of the ovpn files. The file determines the location of the server that your VPN router will pass traffic through. These directions are assuming that you download one of the tcp files.
5. Download https://downloads.nordcdn.com/configs/archives/certificates/servers.zip and extract the appropriate .crt and .key file of the same name as the ovpn file previously downloaded. For instance extract al1_nordvpn_com_ca.crt and al1_nordvpn_com_tls.key if you extracted al1.nordvpn.com.tcp443.ovpn in the previous step.
6. Around line 29 you will see a line with <ca> on it. This line and everything after this line should be deleted. Save the file.
7. Find the line that say auth-user-pass and change it to:

```
auth-user-pass key.txt
```

8. Open a text editor such as gedit and enter your username and password. The user name must go on the first line followed by the password on the next. The user name is probably the email address you used to sign up and the password can be set/found in an email sent by NordVPN following sign up. The email is titled “NordVPN account activation”. Save the file you create below as etc/openvpn/key.txt. Example of the file:

```
user@email.com
JiiF3kWofkF
```

9. Open the etc/config directory and edit the openvpn file in a text editor. Change the following line: option config /etc/openvpn/ to include your opvn file that you downloaded to the etc/openvpn directory in the earlier step. Save file after editing. Example:

```
option config “/etc/openvpn/al1.nordvpn.com.tcp443.ovpn”
```

10. In the etc/openvpn ovpn file you will also need to change the line that reads auth-user-pass to auth-user-pass key.txt
11. Open the librecmc-openvpn-setup directory and right click on the etc folder. You need to “tar it up”. To do that select the Compress option. Then click the Create button and Close button respectively. Make sure the tar.gz option in the drop down is selected for the type of compression.
12. Connect an ethernet cable from the LAN port of the mini VPN router to the ethernet port on your computer. Plug the mini VPN router in.
13. On your computer disconnect from the wifi (if you are connected to an access point)
14. On your computer open a web browser and enter https://192.168.10.1/ into the address bar. Then hit enter.
15. Accept the security warning and continue anyway
16. Click the Login button (you may need to enter 'root' for the user name and 'none' as the password if your changing providers)
17. Click Go to password configuration... link
18. Enter a password in the Password box and again in the Confirmation box. Take note of the router password as you'll need it to configure the router in the future.
19. Scroll down to the bottom of the page and click the Save and Apply button. Wait a few moments for changes to take affect.
20. Go to System > Backup / Flash Firmware
21. Click Browse button under the Backup / Restore section
22. Select the librecmc-openvpn-setup/etc.tar.gz file you created earlier and click the Upload Archive button. Let the router restart. Then login.
23. Set DNS server in Network > Interfaces > WAN > Advanced Settings and enter a DNS. Uncheck Use DNS servers advertised by peer to do this. Enter 84.200.69.80 in the Use custom DNS servers box. Click save.
24. Set the IP to 192.168.3.1 : Network > Interfaces. Next to LAN click Edit. In the IPv4 address change the address to 192.168.3.1. Click Save. Note: If your primary router is using a 192.168.3.x subnet then you will need to change the mini router's subnet to something else.
25. Network > Wireless and click the Edit button next to where it says the SSID name (libreCMC).
Scroll down to the bottom of the page where it says Interface Configuration. Under the General Setup there is a box that says ESSID next to it. Change the name from libreCMC to libreCMC-VPN. Click the Wireless Security tab and enter a password where it says Key. Take note of this. It is the password you'll need to connect to your libreCMC-VPN access point in the steps below. Click Save & Apply button.
26. Give it 30 seconds and switch your ehternet cable from the LAN port on your computer to a LAN port on your primary router. Then the other end to the WAN port on your mini VPN router.
27. You can now turn the mini VPN router off and on again (pull the power on the router and reconnect). Give the mini VPN router a minute or two to boot up.
28. Turn your wifi back on, and select the libreCMC-VPN network from the list of access points. If you did not enter a password for the SSID as instructed above the default password is librecmc. Otherwise enter the password you selected for the SSID to connect. You should now be able to open a browser and confirm that your connected through the VPN by visiting a geolocation service website. Example http://www.infosniper.net/. It should indicate that your visiting from a city, state, and country of the .ovpn file selected earlier.

IVPN Setup Instructions

(this is applicable to users who did not purchase VPN service with router, for generic instruction with other VPN providers see README on CD)

1. To utilize IVPN with our libre router software find your login credentials (probably found in your email or via logging in to the site).
2. Create a folder in your home directory named librecmc-openvpn-setup and copy the Default-VPN-Config.tar.gz file from the included CD to this directory. Extract the files.
3. Create a directory in the etc folder called openvpn.
4.You will need to extract an ovpn config file to your newly created etc/openvpn folder. You can get the zip file containing the ovpn file from: https://www.ivpn.net/releases/config/ivpn-openvpn-config.zip. Note: You can select any of the ovpn files. The file determines the location of the server that your VPN router will pass traffic through. These directions are assuming that you download one of the udp files.
5. Find the line that say auth-user-pass and change it to:

auth-user-pass key.txt

6. Open a text editor such as gedit and enter your username and password. The user name must go on the first line followed by the password on the next. The user name is probably the email address you used to sign up and the password can be set/found in an email sent by IVPN following sign up. The email is titled “IVPN Setup Instructions”. Save the file you create below as etc/openvpn/key.txt. Example of the file:

user@email.com
JiiF3kWofkF

7. Open the etc/config directory and edit the openvpn file in a text editor. Change the following line: option config /etc/openvpn/ to include your opvn file that you downloaded to the etc/openvpn directory in the earlier step. Save file after editing. Example:

option config “/etc/openvpn/Austria.ovpn”

8. In the etc/openvpn ovpn file you will also need to change the line that reads auth-user-pass to auth-user-pass key.txt
9. Open the librecmc-openvpn-setup directory and right click on the etc folder. You need to “tar it up”. To do that select the Compress option. Then click the Create button and Close button respectively. Make sure the tar.gz option in the drop down is selected for the type of compression.
10. Connect an ethernet cable from the LAN port of the mini VPN router to the ethernet port on your computer. Plug the mini VPN router in.
11. On your computer disconnect from the wifi (if you are connected to an access point)
12. On your computer open a web browser and enter https://192.168.10.1/ into the address bar. Then hit enter.
13. Accept the security warning and continue anyway
14. Click the Login button (you may need to enter 'root' for the user name and 'none' as the password if your changing providers)
15. Click Go to password configuration... link
16. Enter a password in the Password box and again in the Confirmation box. Take note of the router password as you'll need it to configure the router in the future.
17. Scroll down to the bottom of the page and click the Save and Apply button. Wait a few moments for changes to take affect.
18. Go to System > Backup / Flash Firmware
19. Click Browse button under the Backup / Restore section
20. Select the librecmc-openvpn-setup/etc.tar.gz file you created earlier and click the Upload Archive button. Let the router restart. Then login.
21. Set DNS server in Network > Interfaces > WAN > Advanced Settings and enter a DNS. Uncheck Use DNS servers advertised by peer to do this. Enter 84.200.69.80 in the Use custom DNS servers box. Click save.
22. Set the IP to 192.168.3.1 : Network > Interfaces. Next to LAN click Edit. In the IPv4 address change the address to 192.168.3.1. Click Save. Note: If your primary router is using a 192.168.3.x subnet then you will need to change the mini router's subnet to something else.
23. Network > Wireless and click the Edit button next to where it says the SSID name (libreCMC).
Scroll down to the bottom of the page where it says Interface Configuration. Under the General Setup there is a box that says ESSID next to it. Change the name from libreCMC to libreCMC-VPN. Click the Wireless Security tab and enter a password where it says Key. Take note of this. It is the password you'll need to connect to your libreCMC-VPN access point in the steps below. Click Save & Apply button.
24. Give it 30 seconds and switch your ehternet cable from the LAN port on your computer to a LAN port on your primary router. Then the other end to the WAN port on your mini VPN router.
25. You can now turn the mini VPN router off and on again (pull the power on the router and reconnect). Give the mini VPN router a minute or two to boot up.
26. Turn your wifi back on, and select the libreCMC-VPN network from the list of access points. If you did not enter a password for the SSID as instructed above the default password is librecmc. Otherwise enter the password you selected for the SSID to connect. You should now be able to open a browser and confirm that your connected through the VPN by visiting a geolocation service website. Example http://www.infosniper.net/. It should indicate that your visiting from a city, state, and country of the .ovpn file selected earlier.

PureVPN Setup Instructions

(this is applicable to users who did not purchase VPN service with router, for generic instruction with other VPN providers see README on CD)

0. To utilize PureVPN with our libre router software find your login credentials (probably found in your email or via logging in to the site).
1. Create a folder in your home directory named librecmc-openvpn-setup and copy the Default-VPN-Config.tar.gz file from the included CD to this directory.
2. Extract the files
3. Visit https://support.purevpn.com/openvpn-files-for-windows-routers-ios-linux-and-mac and select the "Click here to Download File" link next to "Linux". Save the file to your librecmc-openvpn-setup directory.
4. Open the librecmc-openvpn-setup directory and extract the contents of linux-files.zip
5. Open the "Linux OpenVPN Updated files" directory and copy ca.crt and Wdc.key from this directory to your librecmc-openvpn-setup/etc/openvpn directory. Please note this directory does not exist by default. Please create it first.
6. Open the "Linux OpenVPN Updated files/TCP" directory and pick a .opvn file pertaining to the location of the server you would like to connect to. Copy this file to the librecmc-openvpn-setup/etc/openvpn directory.
7. If you have made payment PureVPN will email you VPN Credentials. This will be in an email titled something to the effect of: "RE: PureVPN [One Month Unlimited Plan Account] ***". Open a text editor and copy the VPN Credentials. Do NOT include the actual text "User Name:" or "Password". The first line needs to be the user name and the 2nd line needs to be the password. It should look something like this (but with whatever your user name and password are):

```
purevpn0s24545214
423kegsf
```

Save the file as key.txt in the librecmc-openvpn-setup/etc/openvpn directory.
8. Open the .opvn file in the librecmc-openvpn-setup/etc/openvpn directory and change the line that has auth-user-pass on it to: auth-user-pass key.txt
9. Save it and exit the text editor
10. Open the librecmc-openvpn-setup/etc/config/openvpn file in a text editor and change the line that reads option config /etc/openvpn/USA-NEWYORK-TCP.ovpn to that of the opvn file you have stored in the librecmc-openvpn-setup/etc/openvpn directory. For example I have SWEDEN(V)-TCP.ovpn in my librecmc-openvpn-setup/etc/openvpn directory so I changed this to: option config /etc/openvpn/SWEDEN(V)-TCP.ovpn

Save the file and exit the text editor. Note: Find fastest and least loaded server at https://www.purevpn.com/speed-test

11. Open the librecmc-openvpn-setup directory and right click on the etc folder. You need to "tar it up". To do that select the Compress option. Then click the Create button and Close button respectively. Make sure the tar.gz option in the drop down is selected for the type of compression.
12. Connect an ethernet cable from the LAN port of the mini VPN router to the ethernet port on your computer
13. On your computer disconnect from the wifi (if you are connected to an access point)
14. On your computer open a web browser and enter https://192.168.10.1/ into the address bar. Then hit enter.
15. Accept the security warning and continue anyway
16. Click the Login button (you may need to enter 'root' for the user name and 'none' as the password if your changing providers)
17. Click Go to password configuration... link
18. Enter a password in the Password box and again in the Confirmation box. Take note of the router password as you'll need it to configure the router in the future.
19. Scroll down to the bottom of the page and click the Save and Apply button
20. Go to System > Backup / Flash Firmware
21. Click Browse button under the Backup / Restore section
22. Select the librecmc-openvpn-setup/etc.tar.gz file you created earlier and click the Upload Archive button.
23. Set DNS server in Network > Interfaces > WAN > Advanced Settings and enter a DNS. Uncheck Use DNS servers advertised by peer to do this. Enter 84.200.69.80 in the Use custom DNS servers box.
24. Set the IP to 192.168.3.1 : Network > Interfaces. Next to LAN click Edit. In the IPv4 address change the address to 192.168.3.1. Click Save. Note: If your primary router is using a 192.168.3.x subnet then you will need to change the mini router's subnet to something else.
25. After about 60 seconds you can disconnect the ethernet cable and re-connect it from the WAN port on the mini VPN router to the LAN port on your modem or main router.
26. Go to Network > Wifi and click the Edit button next to where it says the SSID name (libreCMC).
Scroll down to the bottom of the page where it says Interface Configuration. Under the General Setup there is a box that says ESSID next to it. Change the name from libreCMC to libreCMC-VPN. Click the Wireless Security tab and enter a password where it says Key. Take note of this. It is the password you'll need to connect to your libreCMC-VPN access point in the steps below. Click Save & Apply button.
27. Switch your ehternet cable from the LAN port on your computer to a LAN port on your primary router. Then the other end to the WAN port on your mini VPN router.
28. You can now turn the mini VPN router off and on again (pull the power on the router and reconnect). Give the mini VPN router a minute or two to boot up.
29. Turn your wifi back on, and select the libreCMC-VPN network from the list of access points. If you did not enter a password for the SSID as instructed above the default password is librecmc. Otherwise enter the password you selected for the SSID to connect. You should now be able to open a browser and confirm that your connected through the VPN by visiting a geolocation service website. Example http://www.infosniper.net/. It should indicate that your visiting from a city, state, and country of the .ovpn file selected earlier.

PenguinVPN Setup Instructions

(this is applicable to users who did not purchase VPN service with router, for generic instruction with other VPN providers see README on CD)

0. If you didn’t purchase a PenguinVPN subscription step 0 is visiting the networking section at ThinkPenguin.com and selecting a subscription
1. Download https://www.thinkpenguin.com/files/PenguinVPN-default-vpn-configure.tar.gz
2. Open the PenguinVPN-default-vpn-configure.tar.gz file in the archive manager or similar program
3. Browse to the /etc/openvpn directory and open the key.txt file in your favourite text editor
4. In the key.txt file replace the default user name penguin0s1380119 with your VPN user name and default password 6ak2i5b4 with your VPN password
5. Save it and exit the text editor
6. The archive manager will notify you that changes to this file were made and prompt you to save them. Do so.
7. Connect an ethernet cable from the LAN port of the mini VPN router to the ethernet port on your computer
8. On your computer disconnect from the wifi (if you are connected to an access point)
9. On your computer open a web browser and enter https://192.168.10.1/ into the address bar. Then hit enter.
10. Accept the security warning and continue anyway
11. Click the Login button (you may need to enter 'root' for the user name and 'none' as the password if your changing providers)
12. Click Go to password configuration... link
13. Enter a password in the Password box and again in the Confirmation box. Take note of the router password as you'll need it to configure the router in the future.
14. Scroll down to the bottom of the page and click the Save and Apply button
15. Go to System > Backup / Flash Firmware
16. Click Browse button under the Backup / Restore section
17. Select the PenguinVPN-default-vpn-configure.tar.gz file you downloaded and made changes to earlier and click the Upload Archive button.
18. Switch your ehternet cable from the LAN port on your computer to a LAN port on your primary router. Then the other end to the WAN port on your mini VPN router.
19. You can now turn the mini VPN router off and on again (pull the power on the router and reconnect). Give the mini VPN router a minute or two to boot up.
20. Turn your wifi back on, and select the libreCMC-VPN network from the list of access points. The default password is librecmc. Enter this password for the SSID to connect. You should now be able to open a browser and confirm that your connected through the VPN by visiting a geolocation service website. Example http://www.infosniper.net/. It should indicate that your surfing from a different city, state, and country than the one your in.

HideMyAss VPN Setup Instructions

(this is applicable to users who did not purchase VPN service with router, for generic instruction with other VPN providers see README on CD)

1. Locate your HideMyAss VPN credentials. This is the user name and password selected for accessing the HMA web site/control panel (it is the same password you'll use to connect to HMA's OpenVPN servers).
2. Create a folder in your home directory named librecmc-openvpn-setup and copy the Default-VPN-Config.tar.gz file from the included CD to this directory. Extract the files.
3. Create a directory in the etc folder called openvpn.
4.You will need to download an ovpn config file to your newly created etc/openvpn folder. You can get this file from https://www.hidemyass.com/vpn-config/TCP/. Note: You can pick any opvn file you like. Each opvn file contains information on the server your connecting to and its location.
5. Open a text editor such as gedit and enter your username and password. The user name must go on the first line followed by the password on the next. This is the user name and password selected when signing up for HMA service in the prior step. Then save file. Example:

thinkpenguin
4yamDi3gf1

6. Open the etc/config directory and edit the openvpn file in a text editor. Change the following line: option config /etc/openvpn/ to include your opvn file that you downloaded to the etc/openvpn directory in the earlier step. Save file after editing. Example:

option config /etc/openvpn/USA.Florida.Jacksonville_LOC1S1.TCP.ovpn

7. In the etc/ ovpn file you will also need to change the line that reads auth-user-pass to auth-user-pass key.txt
8. Open the librecmc-openvpn-setup directory and right click on the etc folder. You need to “tar it up”. To do that select the Compress option. Then click the Create button and Close button respectively. Make sure the tar.gz option in the drop down is selected for the type of compression.
9. Connect an ethernet cable from the LAN port of the mini VPN router to the ethernet port on your computer
10. On your computer disconnect from the wifi (if you are connected to an access point)
11. On your computer open a web browser and enter https://192.168.10.1/ into the address bar. Then hit enter.
12. Accept the security warning and continue anyway
13. Click the Login button (you may need to enter 'root' for the user name and 'none' as the password if your changing providers)
14. Click Go to password configuration... link
15. Enter a password in the Password box and again in the Confirmation box. Take note of the router password as you'll need it to configure the router in the future.
16. Scroll down to the bottom of the page and click the Save and Apply button
17. Go to System > Backup / Flash Firmware
18. Click Browse button under the Backup / Restore section
19. Select the librecmc-openvpn-setup/etc.tar.gz file you created earlier and click the Upload Archive button.
20. Set DNS server in Network > Interfaces > WAN > Advanced Settings and enter a DNS. Uncheck Use DNS servers advertised by peer to do this. Enter 84.200.69.80 in the Use custom DNS servers box.
21. Set the IP to 192.168.3.1 : Network > Interfaces. Next to LAN click Edit. In the IPv4 address change the address to 192.168.3.1. Click Save. Note: If your primary router is using a 192.168.3.x subnet then you will need to change the mini router's subnet to something else.
22. After about 60 seconds you can disconnect the ethernet cable and re-connect it from the WAN port on the mini VPN router to the LAN port on your modem or main router.
23. Go to Network > Wifi and click the Edit button next to where it says the SSID name (libreCMC).
Scroll down to the bottom of the page where it says Interface Configuration. Under the General Setup there is a box that says ESSID next to it. Change the name from libreCMC to libreCMC-VPN. Click the Wireless Security tab and enter a password where it says Key. Take note of this. It is the password you'll need to connect to your libreCMC-VPN access point in the steps below. Click Save & Apply button.
24. Switch your ehternet cable from the LAN port on your computer to a LAN port on your primary router. Then the other end to the WAN port on your mini VPN router.
25. You can now turn the mini VPN router off and on again (pull the power on the router and reconnect). Give the mini VPN router a minute or two to boot up.
26. Turn your wifi back on, and select the libreCMC-VPN network from the list of access points. If you did not enter a password for the SSID as instructed above the default password is librecmc. Otherwise enter the password you selected for the SSID to connect. You should now be able to open a browser and confirm that your connected through the VPN by visiting a geolocation service website. Example http://www.infosniper.net/. It should indicate that your visiting from a city, state, and country of the .ovpn file selected earlier.