equinux

VPN Tracker 365

VPN Configuration Guide

DD-WRT

© 2018 equinux AG and equinux USA, Inc. All rights reserved.

Under copyright law, this manual may not be copied, in whole or in part, without the written consent of equinux AG or equinux USA, Inc. Your rights to the software are governed by the accompanying software license agreement.

The equinux logo is a trademark of equinux AG and equinux USA, Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

equinux shall have absolutely no liability for any direct or indirect, special or other consequential damages in connection with the use of this document or any change to the router in general, including without limitation, any lost profits, business, or data, even if equinux has been advised of the possibility of such damages.

Every effort has been made to ensure that the information in this manual is accurate. equinux is not responsible for printing or clerical errors.

Revised 16 October 2018

Apple, the Apple logo, iBook, Mac, Mac OS, MacBook, PowerBook are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

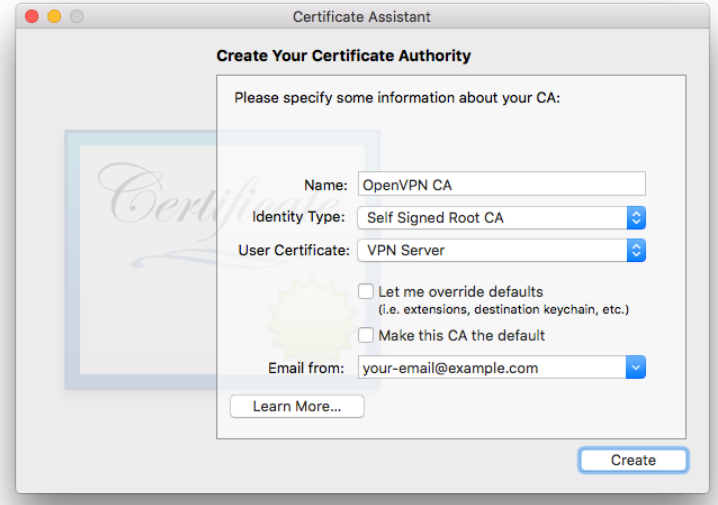
www.equinux.com

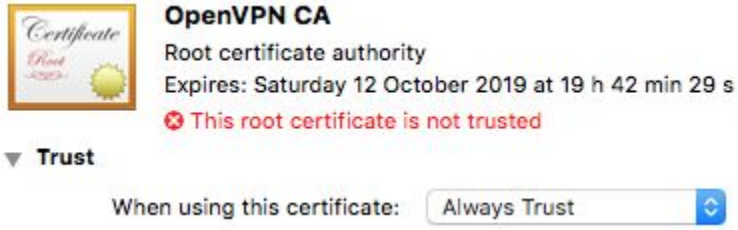
Task One - Setting up the certificates

Step One: Preparing the CA Certificate

A CA (Certificate Authority) certificate is a certificate used to verify the validity of other certificates. The server certificate as well as all the client certificates of your DD-WRT VPN connection need to be signed by a CA certificate, thus this certificate has to be created first.

- ➔ Start the default application “Keychain Access”.
- ➔ From the menu select
  “Keychain Access > Certificate Assistant > Create a Certificate Authority...”.
- ➔ You are free to choose any name and email address for your CA certificate, but you should uncheck “Make this CA the default” and choose “VPN Server” for “User Certificate”.
- ➔ The newly created CA certificate is not trusted by default. Please double click the certificate, open the “Trust” settings and set them to “Always Trust”. As soon as you close that window, the new trust settings will be activated.

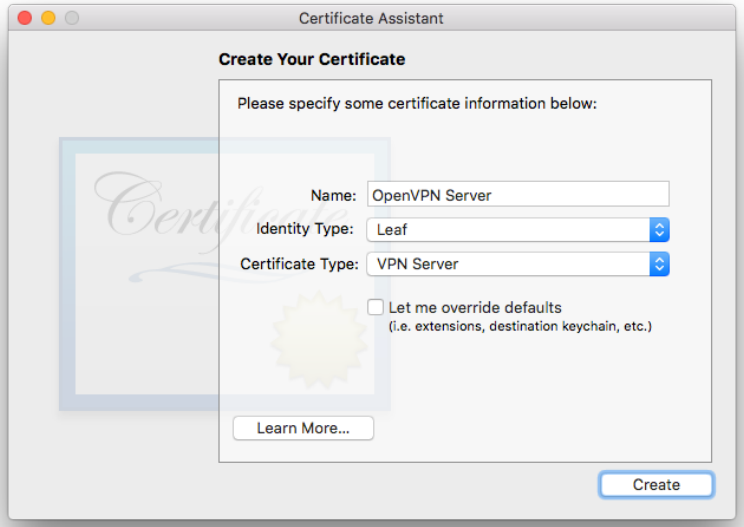




After performing these steps, the resulting entries created in your keychain should look as shown aside:

Step Two: Preparing the server certificate

The server certificate authenticates the VPN server towards its clients. To prove its validity, it has to be signed by the CA certificate created in Step One.



- ➔ Start the default application “Keychain Access”.
- ➔ From the menu select
  “Keychain Access > Certificate Assistant > Create a Certificate...”.
- ➔ You are free to choose any name, but the “Identity Type” must be “Leaf” and the “Certificate Type” should be “VPN Server”.
- ➔ As an issuer, choose the CA certificate created in Step One.

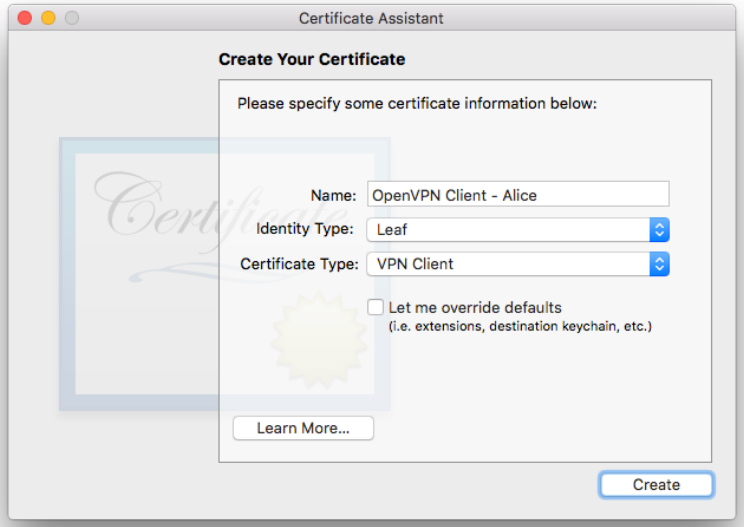
As the CA certificate is no trusted by the system, every certificate you sign with it is automatically trusted as well. Thus at the end of Step Two, your keychain should look similar to the example below:

OpenVPN CA	certificate
OpenVPN CA	public key
OpenVPN CA	private key
OpenVPN Server	public key
OpenVPN Server	private key
OpenVPN Server	certificate

Step Three: Preparing the client certificate

The client certificate authenticates a VPN client towards its VPN server. To prove its validity, it has to be signed by the CA certificate created in Step One.

- ➔ Start the default application “Keychain Access”.
- ➔ From the menu select “Keychain Access > Certificate Assistant > Create a Certificate…”.
- ➔ You are free to choose any name, but the “Identity Type” must be “Leaf” and the “Certificate Type” should be “VPN Client”.
- ➔ As an issuer, choose the CA certificate created in Step One.



As every user of your VPN requires an own client certificate, it is recommended to add the name of the user (here: Alice) to the certificate name so that it is easy to later on distinguish certificates of different users. After completing Step Three, your keychain should contain nine new entries:

OpenVPN CA	certificate
OpenVPN CA	public key
OpenVPN CA	private key
OpenVPN Client - Alice	public key
OpenVPN Client - Alice	private key
OpenVPN Client - Alice	certificate
OpenVPN Server	public key
OpenVPN Server	private key
OpenVPN Server	certificate

Task Two - Preparing the files

Step One: Exporting the CA certificate

- ➔ Start the default application “Keychain Access”.
- ➔ Select the CA certificate.
- ➔ From the menu select “File > Export Items...”.
- ➔ Make sure the export format is set to “Privacy Enhanced Mail (.pem)”

Step Two: Exporting the server certificate

- ➔ Start the default application “Keychain Access”.
- ➔ Select the server certificate.
- ➔ From the menu select “File > Export Items...”.
- ➔ Make sure the export format is set to “Privacy Enhanced Mail (.pem)”

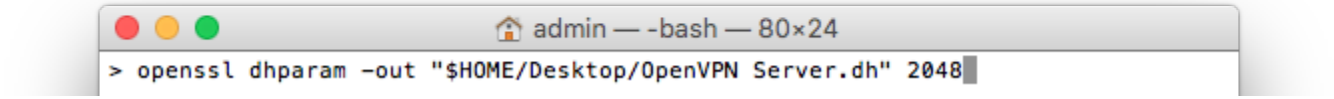
Step Three: Exporting the server private key

- ➔ Start the default application “Keychain Access”.
- ➔ Select the server private key.
- ➔ From the menu select “File > Export Items...”.
- ➔ The only format allowed for exporting is “Personal Information Exchange (.p12)”.
- ➔ When prompted for a password to protect the exported data, you are free to choose any password you like.

Step Four: Creating the DH parameters

- ➔ Start the default application “Terminal”.
- ➔ Copy and paste the following command to the terminal window:

```
openssl dhparam -out "$HOME/Desktop/OpenVPN Server.dh" 2048
```



- ➔ Press Return to activate it.

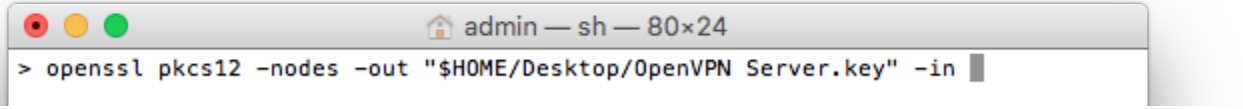
The command will run for a while, calculating a very large prime number, which is a rather expensive computation and depending on the speed of your system it can really take a while, so please be patient. Once done, a new file named “OpenVPN Server.dh” will appear on your Desktop.

Step Five: Convert the server private key

For security reasons, the Keychain Access only allows you to export private keys to the PKCS #12 file format (.p12) , since that is the only file format that protects keys by an additional layer of encryption. Yet the DD-WRT OpenVPN server requires the private key in PEM format, just like its certificates. Thus the exported key requires a manual conversion.

- ➔ Start the default application “Terminal”.
- ➔ Copy and paste the following command to the terminal window, but don’t activate it by pressing return:

```
openssl pkcs12 -nodes -out "$HOME/Desktop/OpenVPN Server.key" -in
```



- ➔ Make sure there is at least one space after “-in”.
- ➔ Drag and drop the private key file from Step Three onto the Terminal window. The path to the file is appended to the command.
- ➔ Press Return to activate the command.
- ➔ When prompted, enter the password you chose during export in Step Three. (Be aware: There is no visible typing)

Once the command finished processing, a new file named “OpenVPN Server.key” will appear on your Desktop.

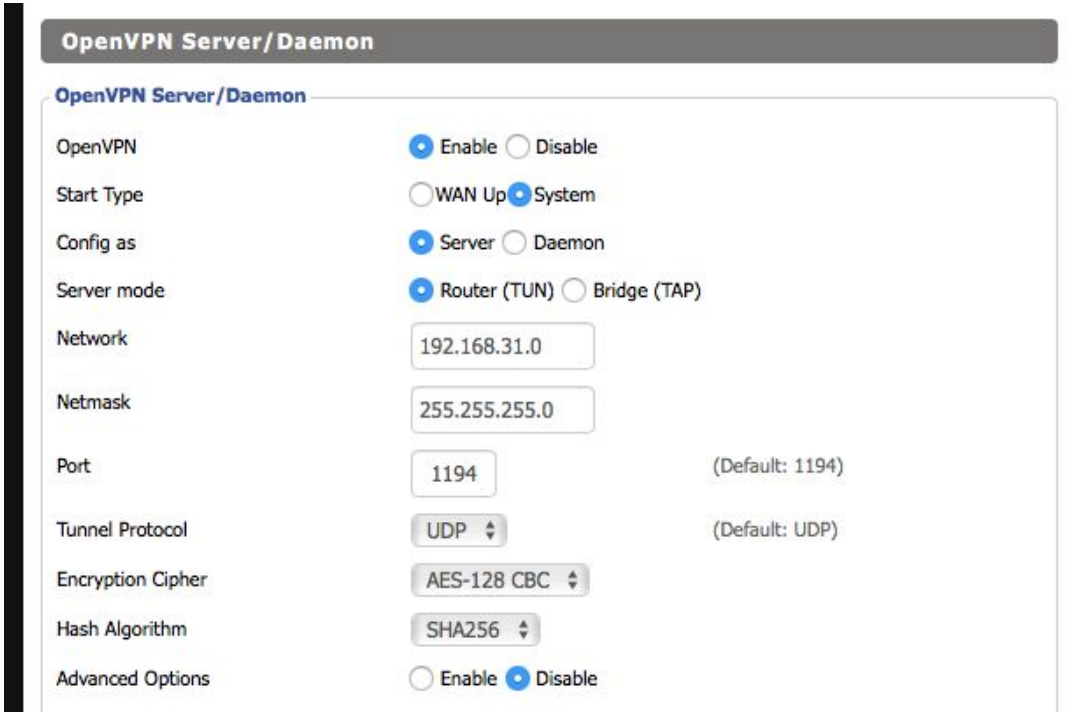
Step Six: Gathering all the files together

After successfully performing all the other steps above, you should have the following four files available:

These files are required during Task Three when setting up the OpenVPN server, their content will be transferred to your DD-WRT setup. If you cannot perform this setup from your current Mac, please be sure to transfer the files as secure as possible (e.g. consider using an USB stick for transfer) because none of them has any layer of protection anymore. Especial the private key and the DH file are essential for the security of your VPN setup.

Task Three - Setting up the server

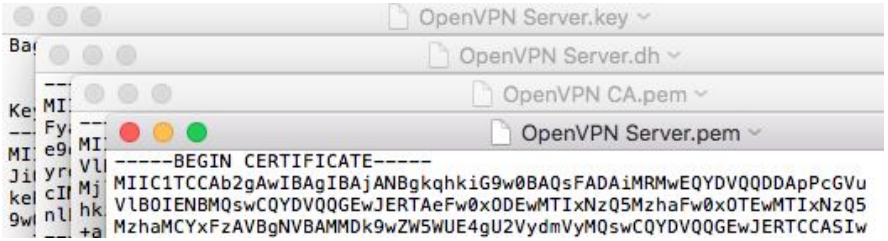
Step One: Creating the OpenVPN setup



- ➔ Connect to your DD-WRT gateway.
- ➔ Navigate to “Services > VPN”.
- ➔ Enable OpenVPN.
- ➔ Set “Start Type” to “System”.
- ➔ Set “Config as” to “Server”.
- ➔ Set “Server Mode” to “Router (TUN)”.
- ➔ “Network” and “Netmask” define a network from that IP addresses are assigned to the VPN users. You are free to choose **any private IP network** here as long as it **does not collide with any DMZ/LAN network** configured on your DD-WRT router. 192.168.31.0 is only a sample value and we do not imply or recommend that you also use this value in your setup.
- ➔ We recommend to keep the default “Port” value of “1194”.
- ➔ We recommend to keep the default “Tunnel Protocol” as “UDP” offers the best VPN performance.
- ➔ We recommend to choose “AES-128 CBC” as “Encryption Cipher” and “SHA256” as Hash Algorithm, since this combination provides by far the best trade-off between performance and security.

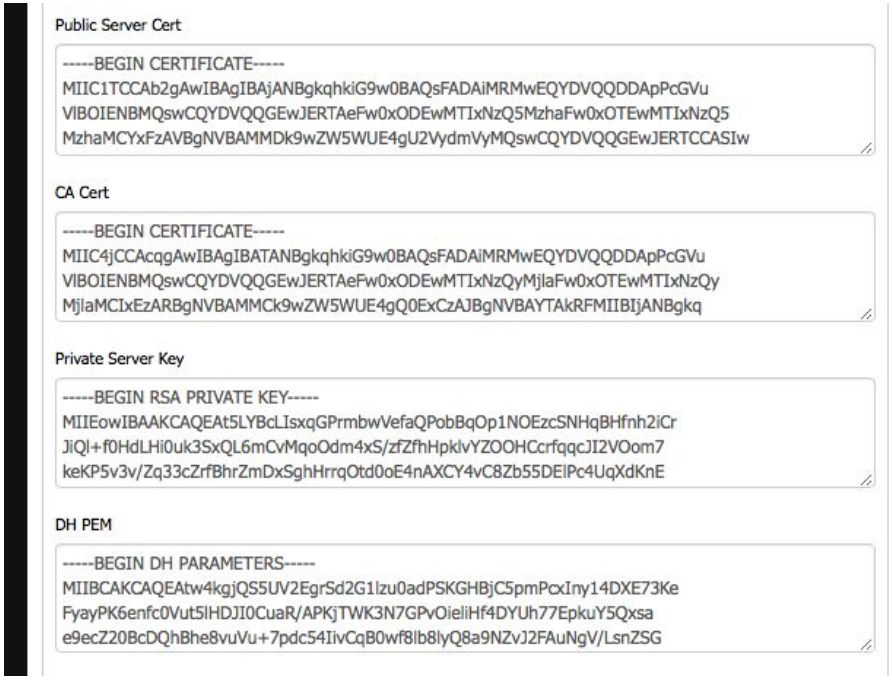
Step Two: Transferring the files

All the files that have been collected at the end of Task Two contain human readable text. You can open them with any text editor of your choice, e.g. just start the default app “TextEdit” and simply drag and drop all these files onto its Dock icon.



Every file has a line stating “`----- BEGIN <something> -----`” and “`----- END <something> ----`”. The content in-between these two lines, *including the lines themselves*, need to be transferred to your DD-WRT router.

- ➔ Copy and paste the server certificate to “Public Server Cert”.
- ➔ Copy and paste the CA certificate to “CA Cert”.
- ➔ Copy and paste the private key to “Private Server Key”.
- ➔ Copy and paste the DH parameters to “DH PEM”.
- ➔ Finally click “Apply Settings”.



Task Four - Setting up VPN Tracker

Step One: Add a connection

- ➔ Open VPN Tracker 365.
- ➔ Click on “Create a connection”, or click on the + in the bottom left corner of the app window.
- ➔ Select “DD-WRT > OpenVPN”
- ➔ Click “Create.”

Step Two: Configure the VPN connection for your device

- ➔ Click on “Configure” and go to the “Basic” tab.
- ➔ Enter the public (WAN) IP address or DNS name of your DD-WRT router in the field “VPN Gateway”.
- ➔ List all LAN/DMZ networks you wish to access over the VPN as “Additional Remote Networks”. Once the connection is up, you will only have access to the network addresses listed here.
- ➔ Click on “No certificate selected”.
- ➔ Select the client certificate as “Local Certificate”.
- ➔ Select the CA certificate as “Remote CA”.
- ➔ Click “OK”.

Task Five - Testing the VPN connection

In order to test your connection, you will need to connect from a different Internet connection than the one the gateway is using. For example, if you are setting up a VPN connection to your office, try it out at home, from an Internet cafe, or use your mobile phone as your own personal hotspot.

Connect to your VPN

- ➔ Check first of all that your internet connection is working as it should be. Use this link as a test: http://www.equinux.com
- ➔ Start the VPN Tracker 365 app.
- ➔ Click on the On/Off slider to turn on your connection.

IMPORTANT:

If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection. Wait for the test to complete.

Connected!

Connecting may take a couple of seconds. If the On/Off button turns blue that's great – you're connected! Now is a great time to take a look at the VPN Tracker Manual. It shows you how to use your VPN and how to get the most out of it.

Troubleshooting

In case there's a problem connecting, a yellow warning triangle will show up. Click the yellow warning triangle to be taken to the log. The log will explain exactly what the problem is. Follow the steps listed in the log.
TIP: Press Cmd-L to open the log in a new window. That way, you can have the log side-by-side with your VPN configuration while making changes to troubleshoot a problem.

VPN Tracker Manual

The VPN Tracker Manual contains detailed troubleshooting advice. Answers to frequently asked questions (FAQs) can be found at: http://www.vpntracker.com/support

Technical Support

If you're stuck, the technical support team at equinux is here to help. Contact us via http://www.vpntracker.com/support

Please include the following information with any request for support:

- ➔ A description of the problem and any troubleshooting steps that you have already taken.
- ➔ A VPN Tracker Technical Support Report (Log > Technical Support Report).
- ➔ Device vendor, model, and DD-WRT version running on it.
- ➔ Screenshots of the VPN settings on your VPN gateway.

IMPORTANT: A Technical Support Report contains the settings and logs necessary for resolving technical problems. Confidential information (e.g. passwords, private keys for certificates) is not included in a Technical Support Report.

Task Six - Adding another VPN user

Step One: Creating a certificate

To add another VPN user, simply repeat the steps of Task Two, Step Three because every VPN users needs an own set of private key and certificate that is signed by the CA certificate you created in Task Two, Step One.

Step Two: Deploying the certificate

- ➔ Start the default application “Keychain Access”.
- ➔ Select both, the certificate and the private key of the user at the same time.
- ➔ From the menu select “File > Export Items...”.
- ➔ Make sure the selected file format is “Personal Information Exchange (.p12)”.
- ➔ Enter a password to protect the private key information.

Step Three: Importing the private key and the certificate

- ➔ On the target Mac, double click the PKCS #12 (.p12) file.
- ➔ Enter the password chosen during export.

Step Four: Setting up VPN Tracker

The required steps to setup VPN Tracker are identical to the ones found Task Four, only a different certificate has to be chosen.

Additional Information

Security considerations

Certificates contain only public information and can only be used to encrypt data and to verify signatures. To decrypt data and to create signatures, the private key is required and as the name implies, this key must be kept private because the security of your VPN raises and falls with the protection level of this key. Never send the password for an encrypted private key over the same communication channel as the private key itself.

Certificate lifetimes

Certificates are only valid for a limit amount of time. By default macOS chooses a time period of one year. After that time period, the certificates become invalid and need to be renewed. If you wish or require longer lifetimes, you can specify your own lifetime by selecting “Let me override defaults” when creating certificates.

Public keys

During the setup process, macOS has to create several key pairs, each one consisting out of a public and a private key. The public key is also wrapped into a certificate. The public key object created serves no purpose for your VPN, so feel free to delete it, to avoid cluttering up your keychain. Only the certificate and the private key are required for the setup.

Gateways with dynamic IP addresses

During Task Four, Step Two you had to enter the public WAN interface IP address of your DD-WRT gateway in VPN Tracker. Please note that unless your service provider offers you a “static IP address”, this IP address is subject to change at any time.

The easiest way to prevent this is to obtain a static IP address, or to setup a dynamic DNS (DDNS) name instead. Log in to your DD-WRT router and go to “Setup > DDNS”. You can choose among a wide variety of supported services to choose from. Once registered at a DDNS service and configured in DD-WRT, there will be a domain name that always resolves to the correct IP address of your DD-WRT gateway. In VPN Tracker you can simply enter the DDNS name instead of an IP address into the “VPN Gateway” field.