

iVPN Help

MacServe

Alex Jones

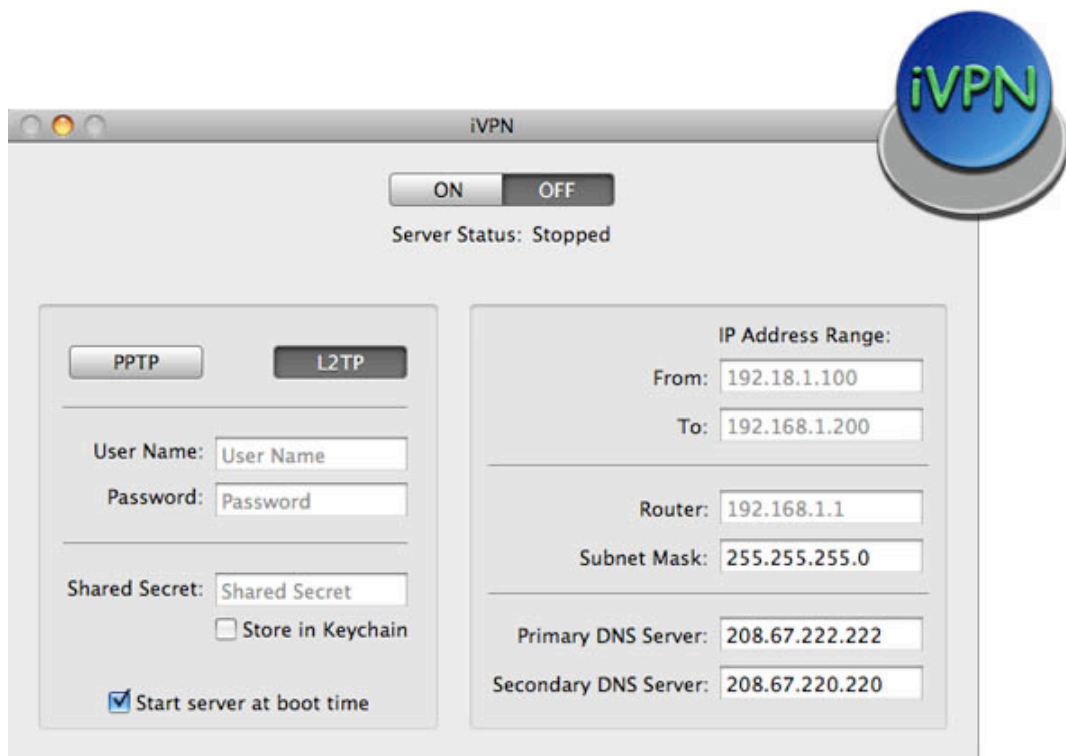


Table of Contents

About.....	3
Company Info	3
Donations	3
How It Works	4
Settings Files.....	4
General Help	5
Starting the server.....	5
Stopping the server.....	5
Starting the server at boot time.....	5
Uninstalling iVPN.....	5
Server Settings	6
VPN Type.....	6
Username and Password.....	6
Shared Secret.....	6
IP Address Range	6
Router	6
Subnet Mask.....	6
Primary and Secondary DNS Servers.....	6
Port Forwarding	7
PPTP Client Settings	8
Configuring the PPTP VPN client on Leopard	8
Configuring the PPTP VPN client on Tiger.....	8
Configuring the PPTP VPN client on iPhone	9
Configuring the PPTP VPN client on Windows XP	9
L2TP IPsec Client Settings.....	10
Configuring the L2TP IPsec VPN client on Leopard	10
Configuring the L2TP IPsec VPN client on Tiger.....	10
Configuring the L2TP IPsec VPN client on iPhone	11
Configuring the L2TP IPsec VPN client on Windows XP	11
Troubleshooting.....	12
I can't connect	12
I can't access the remote network's resources	12
Open Source Licence	13

About

iVPN is an application that makes use of the standards based PPTP and L2TP IPSec VPN server installed with Mac OS X. This VPN server is usually only available on Mac OS X Server and configured through the Server Admin application. iVPN makes it possible to use the same server utility on the client version of Mac OS X.

All you have to do to set it up is to enter the user name and password that you want your VPN clients to use, the IP address range you want to give to your clients and then click start server. iVPN will handle all the other settings and start the VPN server.

iVPN is the GUI that Apple left out.

Company Info

Company website: <http://www.macserve.org.uk/>

Product website: <http://www.macserve.org.uk/projects/ivpn/>

SourceForge.net project page: <http://www.sourceforge.net/projects/ivpnd/>

Support email: admin@macserve.org.uk

Donations

If you like this application and find it useful, please consider making a donation. I have worked hard on this project and have put a lot of effort and time into making the application as good as I possibly can. The time I have spent on developing my application should have been going towards my education. So, any donations made will go toward developing my applications and furthering my knowledge in the field of computer programming.

You can make a donation by either visiting my website and click on one of the 'Donate' buttons. This will redirect you to a secure PayPal website, where you can donate as much or as little as you want using credit/debit card or any other method supported by PayPal. Or, you can visit my SourceForge.net project page and click on 'Donate', where you can choose how much you would like to donate, again, using PayPal.

All donations are greatly appreciated! Thank you!

How It Works

iVPN uses the built-in VPN capabilities of Mac OS X. The VPN server Mac OS X uses is called `vpnd`, an open source UNIX application that is very stable. This same application is used in Apple's very own Mac OS X Server. Obviously, Apple have not included the software needed to configure the VPN server in Mac OS X Client because it would give people one less reason to buy Mac OS X Server.

Settings Files

After you click 'ON', iVPN takes all the settings you entered and puts them into the appropriate files. These files are the only change that iVPN makes to your system.

- All the configuration goes into a file called 'com.apple.RemoteAccessServer.plist'. This file tells how the VPN server should operate. This file is found at `/Library/Preferences/SystemConfiguration`.
- Your Username and Password get put into a file called 'chap-secrets', which is accessed every time someone tries to connect to the server. This file is found at `/private/etc/ppp`.
- If you chose to start the server at boot time, iVPN will place a folder called iVPN in the folder `/Library/StartupItems`. The files contained within this folder are accessed when you start your computer.
- If you use L2TP IPsec and to use the Keychain, iVPN will create a keychain item in the System keychain that is accessed by a UNIX app called 'racon' that handles IPsec authentication.

WARNING :-

DO NOT USE iVPN ON MAC OS X SERVER, YOU WILL NOT BE ABLE TO CONFIGURE YOUR VPN SERVER THROUGH SERVER ADMIN!

General Help

Starting the server

1. Enter a user name and password; the clients connecting to the server will use these.
2. Enter an IP address range (e.g. From: 192.168.1.100, To: 192.168.1.200). This will determine what IP address is given to your clients.
3. Enter the IP address of your router. If you do not have one leave this blank.
4. Choose at least one VPN type, PPTP or L2TP IPsec. If you choose L2TP, enter a shared secret and choose whether or not to store it in the keychain (this sometimes does not work so try running iVPN with and without this option).
5. Leave the other settings as default unless you know of any specific reason why you should change them.
6. Click 'ON'

Stopping the server

1. Open iVPN and click 'OFF' - you will be asked for an administrator password.
2. You can also stop the server manually by killing the 'vpnd' process from Activity Monitor or the Terminal.

Starting the server at boot time

If you would like the server to automatically start when turning on your computer, check this option. You will be asked for a password and then it is done.

Note: You have to have started the server at least once before using this option.

Uninstalling iVPN

Delete the following files:-

- /Applications/iVPN.app
- /Library/Preferences/SystemConfiguration/com.apple.RemoteAccessServers.plist
- /private/etc/ppp/chap-secrets
- A keychain item called 'com.apple.net.racoon' in the System keychain

Server Settings

VPN Type

Choose at least one VPN type, PPTP or L2TP to determine which type of VPN server to run. L2TP is typically more secure so it is advised to use this. But, PPTP is more stable when run from iVPN. You may find it useful to run both.

Username and Password

The username and password you enter does not have to be your accounts. This is completely separate and is only used for your clients to authenticate when connecting.

Shared Secret

You have to enter this if you chose to use L2TP IPsec. This secret is just a password that is used to encrypt your connections. Make sure you use something complex but memorable. E.g. Smith1+john2@ivpn.maC. The shared secret can be stored in the keychain but this does not work on certain systems.

IP Address Range

This section allows you to designate a range of IP address for all of your clients. This can be any valid IP range (e.g. 192.168.1.100 to 192.168.1.200). In this case, when the first client connects, they would get the first available IP address, which would be 192.168.1.100. When the next client connects they would get 192.168.1.101, etc.

Router

This is just the IP address of the router you use. If you do not have one, leave this blank.

Subnet Mask

Unless you know what you're doing, leave this at its default (255.255.255.0).

Primary and Secondary DNS Servers

Unless you have specific DNS servers you would like to assign to your clients, leave these at their defaults (208.67.222.222, 208.67.220.220).

Port Forwarding

To allow clients to connect to your VPN server certain ports need to be open to the Internet. If you have any sort of firewall such as a router, or other software firewall including Mac OS X's built in firewall you will need to specifically tell the firewall to accept incoming connections on these ports.

For PPTP connections, TCP port 1723 needs to be opened.

For L2TP connections UDP port 4500 and 500 need to be opened.

So, on your router, tell it to forward the relevant ports to the IP address of your computer running iVPN. Also, some routers have an option to allow a VPN pass-through. If your router has this functionality, make sure you enable the relevant pass-through.

You will have to enable the appropriate VPN pass-through on the client-side's router also, otherwise negotiation will fail or hang on the client.

For specific help on forwarding ports on your router, refer to your routers instruction manual.

Note: Some of you may think that port 1701 should need to be opened to allow L2TP connections. This is not true. When using L2TP IPSec, the first connection is the IPSec, which uses ports 4500 and 500. Once IPSec is established, L2TP is connected through the encrypted IPSec tunnel on port 500.

PPTP Client Settings

All Mac OS X clients will need to make sure their VPN configuration is top in the network service order in 'Network' in 'System Preferences'. This makes sure all network traffic is routed through the VPN connection.

Configuring the PPTP VPN client on Leopard

1. Open 'System Preferences'
2. Click on 'Network'
3. Click the '+' button
4. Choose 'VPN' as the interface
5. Choose 'PPTP' as the VPN type and name the service whatever you like
6. Click 'Create'
7. Enter the 'Server Address' of your computer running iVPN
8. Enter the username you entered in iVPN in the 'Account Name' field
9. Choose 'Maximum (128 bit only)' for the Encryption
10. Click on 'Authentication Settings...'
11. Make sure 'Password' is chosen and enter the password you entered in iVPN then click 'OK'
12. Choose whatever options you want in 'Advanced...'
13. Click 'Apply'
14. Click 'Connect'

Configuring the PPTP VPN client on Tiger

1. Open 'Internet Connect'
2. Click on the 'VPN' tab
3. Choose 'PPTP' and click 'Continue'
4. Choose 'Edit Configurations...' from the 'Configuration' drop down box
5. Name the connection in the 'Description' field
6. Enter the 'Server Address' of your computer running iVPN
7. Enter the username you entered in iVPN in the 'Account Name' field
8. Make sure 'Password' is chosen for 'User Authentication' and enter the password you entered in iVPN
9. Choose 'Maximum (128 bit only)' for the Encryption
10. Click 'OK'
11. Click 'Connect'

Configuring the PPTP VPN client on iPhone

1. From the home screen, tap on 'Settings', scroll down to 'General' then tap on 'Network'.
2. Tap on 'VPN' then 'Settings'
3. Choose 'PPTP'
4. Enter the address of your computer running iVPN in the 'Server' field
5. Enter the username you entered in iVPN in the 'Account' field
6. Make sure 'RSA SecurID' is turned 'OFF'
7. Enter the password you entered in iVPN in the 'Password' field
8. Choose 'Maximum' for the 'Encryption Level'
9. Turn 'Send all traffic' ON
10. Leave the 'Proxy' off unless you know of any reason for you to use one.
11. Tap 'Save'
12. Use the ON/OFF slider to control the VPN connection either from this menu or from the main 'Settings' menu

Configuring the PPTP VPN client on Windows XP

1. Click on 'Start' then 'Control Panel'
2. Double click on 'Network Connections'
3. Click on 'Create a new connection'
4. Click 'Next'
5. Choose 'Connect to the network at my workplace' then click 'Next'
6. Choose 'Virtual Private Network connection' then click 'Next'
7. Choose a name for the connection and click 'Next'
8. Enter the address of your computer running iVPN then click 'Next'
9. Choose 'Anyone's use' then click 'Next'
10. Click 'Finish'
11. Right click on the connection you just made and choose 'Properties'
12. In the 'Networking' tab, choose 'PPTP' from the 'Type of VPN' drop down box
13. Click 'OK'
14. Double click on the connection you made
15. Enter the username you entered in iVPN in the 'User name' field
16. Enter the password you entered in iVPN in the 'Password' field
17. Choose to save this user name and password
18. Click 'Connect'

L2TP IPsec Client Settings

Configuring the L2TP IPsec VPN client on Leopard

1. Open 'System Preferences'
2. Click on 'Network'
3. Click the '+' button
4. Choose 'VPN' as the interface
5. Choose 'L2TP over IPsec' as the VPN type and name the service whatever you like
6. Click 'Create'
7. Enter the 'Server Address' of your computer running iVPN
8. Enter the username you entered in iVPN in the 'Account Name' field
9. Click on 'Authentication Settings...'
10. Make sure 'Password' is chosen for User Authentication and enter the password you entered in iVPN
11. Make sure 'Shared secret' is chosen for Machine Authentication and enter the shared secret you entered in iVPN then click 'OK'
12. Choose whatever options you want in 'Advanced...'
13. Click 'Apply'
14. Click 'Connect'

Configuring the L2TP IPsec VPN client on Tiger

1. Open 'Internet Connect'
2. Click on the 'VPN' tab
3. Choose 'L2TP IPsec' and click 'Continue'
4. Choose 'Edit Configurations...' from the 'Configuration' drop down box
5. Name the connection in the 'Description' field
6. Enter the 'Server Address' of your computer running iVPN
7. Enter the username you entered in iVPN in the 'Account Name' field
8. Make sure 'Password' is chosen for 'User Authentication' and enter the password you entered in iVPN
9. Make sure 'Shared secret' is chosen for Machine Authentication and enter the shared secret you entered in iVPN
10. Click 'OK'
11. Click 'Connect'

Configuring the L2TP IPsec VPN client on iPhone

1. From the home screen, tap on 'Settings', scroll down to 'General' then tap on 'Network'.
2. Tap on 'VPN' then 'Settings'
3. Choose 'L2TP'
4. Enter the address of your computer running iVPN in the 'Server' field
5. Enter the username you entered in iVPN in the 'Account' field
6. Make sure 'RSA SecurID' is turned 'OFF'
7. Enter the password you entered in iVPN in the 'Password' field
8. Enter the shared secret you entered in iVPN in the 'Secret' field
9. Turn 'Send all traffic' ON
10. Leave the 'Proxy' off unless you know of any reason for you to use one.
11. Tap 'Save'
12. Use the ON/OFF slider to control the VPN connection either from this menu or from the main 'Settings' menu

Configuring the L2TP IPsec VPN client on Windows XP

1. Click on 'Start' then 'Control Panel'
2. Double click on 'Network Connections'
3. Click on 'Create a new connection'
4. Click 'Next'
5. Choose 'Connect to the network at my workplace' then click 'Next'
6. Choose 'Virtual Private Network connection' then click 'Next'
7. Choose a name for the connection and click 'Next'
8. Enter the address of your computer running iVPN then click 'Next'
9. Choose 'Anyone's use' then click 'Next'
10. Click 'Finish'
11. Right click on the connection you just made and choose 'Properties'
12. In the 'Networking' tab, choose 'L2TP IPsec' from the 'Type of VPN' drop down box
13. In the 'Security' tab, click on 'IPsec Settings...', make sure the 'Use pre-shared key for authentication' is checked and enter the shared secret you entered in iVPN then click 'OK'.
14. Click 'OK'
15. Double click on the connection you made
16. Enter the username you entered in iVPN in the 'User name' field
17. Enter the password you entered in iVPN in the 'Password' field
18. Choose to save this user name and password
19. Click 'Connect'

Troubleshooting

I can't connect

If you cannot connect to the server running iVPN from your client make sure you have done the following:

- Forwarded TCP port 1723 for PPTP, or UDP port 4500 and 500 for L2TP IPsec, through any firewalls you may have, this includes Mac OS X's built-in software firewall and any NATs or routers you may have. Please read your router's manual on how to forward ports. Also, some routers have a VPN pass-through feature; if you have this, make sure you enable PPTP or L2TP and IPsec pass-through on both the client-side router and server-side router. To check that ports are open, search Google for an open port checker.
- Check that 'Activity Monitor' lists the process 'vpnd' (and 'racoon' if L2TP IPsec was chosen). If not, email me with your situation.
- Check that you do not have any other software or hardware that could interfere with the VPN server.
- Make sure you have entered the settings correctly in your client.

I can't access the remote network's resources

If you can't connect to any network resources from the connected client such as computers, servers, printers, NAS or the Internet, check the following:

- Check that Internet Sharing is not turned on; this can interfere with the NAT provided to VPN clients.
- Make sure you have entered the IP settings correctly in iVPN.

Open Source Licence

Copyright (c) 2008, Alex Jones

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of MacServe nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.