VPN Configuration Guide

Cisco Small Business (Linksys)
WRV210

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 configuration guide is accurate. equinux is not responsible for printing or clerical errors.

Configuration guide revision 1

Created using Apple Pages.

www.equinux.com

Contents

Introduction

This configuration guide helps you configure VPN Tracker and your Cisco VPN gateway to establish a VPN connection between them.

Using the Configuration Guide

Part 1 – VPN Gateway Configuration

The first part of this guide will show you how to configure a VPN tunnel on your Cisco VPN gateway device using the web configuration interface.

⚠ This guide is a supplement to the documentation included with your Cisco VPN gateway device, it can't replace it. Please read this documentation before starting.

Part 2 – VPN Tracker Configuration

In the second part, this guide will show you how to configure VPN Tracker to easily connect to your newly created VPN tunnel.

Part 3 – Troubleshooting and Supporting Multiple Users

Troubleshooting advice and information on supporting multiple users can be found in the final part of this guide.

💡 If you are setting up VPN on your device for the first time, we strongly recommend you keep to the tutorial-style setup in the first and second part of this document and make modifications only after you have tested the basic setup.

Conventions Used in This Document

Links to External Websites

Sometimes you will be able to find more information on external websites. Clicking links to websites will open the website in your web browser:

http://equinux.com

Links to Other Parts of this Guide

A → *Link* will take you to another place in the configuration guide. Simply click it if you are reading this guide on your computer.

Tips and Tricks

💡 This configuration guide contains lots of great tips. You can easily spot them by looking for the light bulb icon.

Warnings

⚠ This exclamation mark warns you when there is a setting or action where you need to take particular care.

Getting Help

VPN Tracker makes VPN simple. However, computer networking and VPNs can be complex and tricky at times, so we have also built in tools and helpful features that will assist you if you ever run into problems. Check out → *Troubleshooting* for more information.

Prerequisites

Your VPN Gateway

- This guide applies to Cisco Small Business (formerly Linksys) WRV210 routers
- Make sure you have the **latest firmware** version installed that is available for your device. This configuration guide was created using a Cisco WRV210 running firmware v2.0.0.11

Your Mac

VPN Tracker runs on Mac OS X 10.4, 10.5 and 10.6

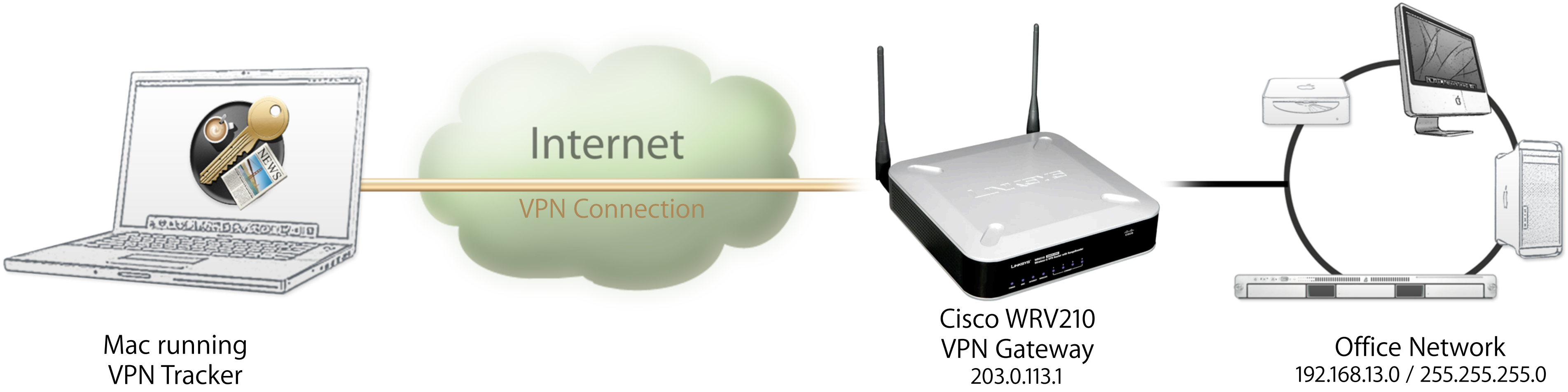
The configuration described in this guide requires VPN Tracker 6. Make sure you have all available updates installed. The latest VPN Tracker updates can always be obtained from http://www.vpntracker.com

Scenario

In our example, we need to connect an employee's Mac to an office network. The diagram on the bottom of this page illustrates this scenario.

This guide assumes that the Mac running VPN Tracker already has internet connectivity. The office's Cisco VPN gateway device (the "VPN gateway") is also already connected to the Internet and can be accessed through a static IP address or DNS host name. In our example setup, we will be using a static IP address: 203.0.113.1.

The VPN gateway has a second network interface which is connected to the internal office network (LAN). In our example, the office network is using the network 192.168.13.0/24 (which is the same as 192.168.13.0/255.255.255.0). This is the network that will be accessed from the employee's Mac through the VPN. It is called the "Remote Network" in VPN Tracker.



Terminology

A VPN connection is often called a "tunnel" (or "VPN tunnel"). Every VPN tunnel is established between two "endpoints". In our example one endpoint is VPN Tracker and the other endpoint is the VPN gateway. Each endpoint is called the other endpoint's "peer".

Please note that for each endpoint, the settings on the other endpoint are considered to be "remote", while its own settings are considered to be "local". That means a "local" setting from VPN Tracker's perspective, is a "remote" setting from the VPN gateway's perspective, and vice versa.

The sample configuration described in this guide is called a "Host to Network" configuration: a single computer, called a "Host" establishes a VPN tunnel to an entire "Network" behind the VPN gateway.

My VPN Gateway Configuration Checklist

Throughout this guide, there are certain pieces of information that are needed later on for configuring VPN Tracker. This information is marked with red numbers to make it easier to reference it later. You can print this checklist to help keep track of the various settings of your VPN gateway device.

IP Addresses

❶ WAN IP Address: ______.______.______.______ (or hostname ____________________________)

❷ LAN Network Address / Subnet Mask: ______.______.______.______ / ______.______.______.______

Pre-Shared Key

❸ Pre-Shared Key: ____________________________

Task 1 – VPN Gateway Configuration

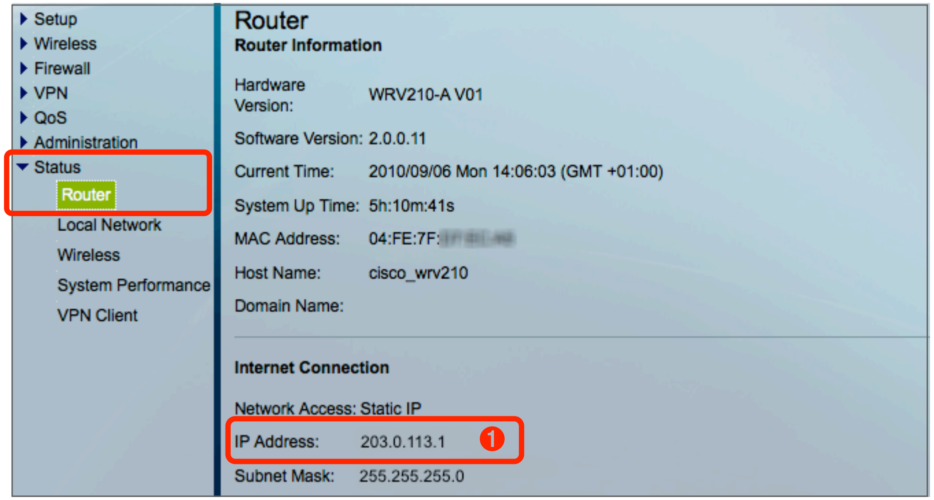
We will first set up VPN on the VPN gateway. If you already have VPN in place, it's helpful to follow along this tutorial to see how settings on the device fit together with VPN Tracker.

Step 1 – Retrieve Network Settings

- Connect to your VPN gateway through its web configuration interface

If you find that the device's web configuration interface is not working properly, you might want to try a different web browser (e.g. Firefox instead of Safari).

- Go to **Status** > **Router**



Router

Router Information

Hardware Version: WRV210-A V01

Software Version: 2.0.0.11

Current Time: 2010/09/06 Mon 14:06:03 (GMT +01:00)

System Up Time: 5h:10m:41s

MAC Address: 04:FE:7F:[redacted]

Host Name: cisco_wrv210

Domain Name:

Internet Connection

Network Access: Static IP

IP Address: 203.0.113.1 ❶

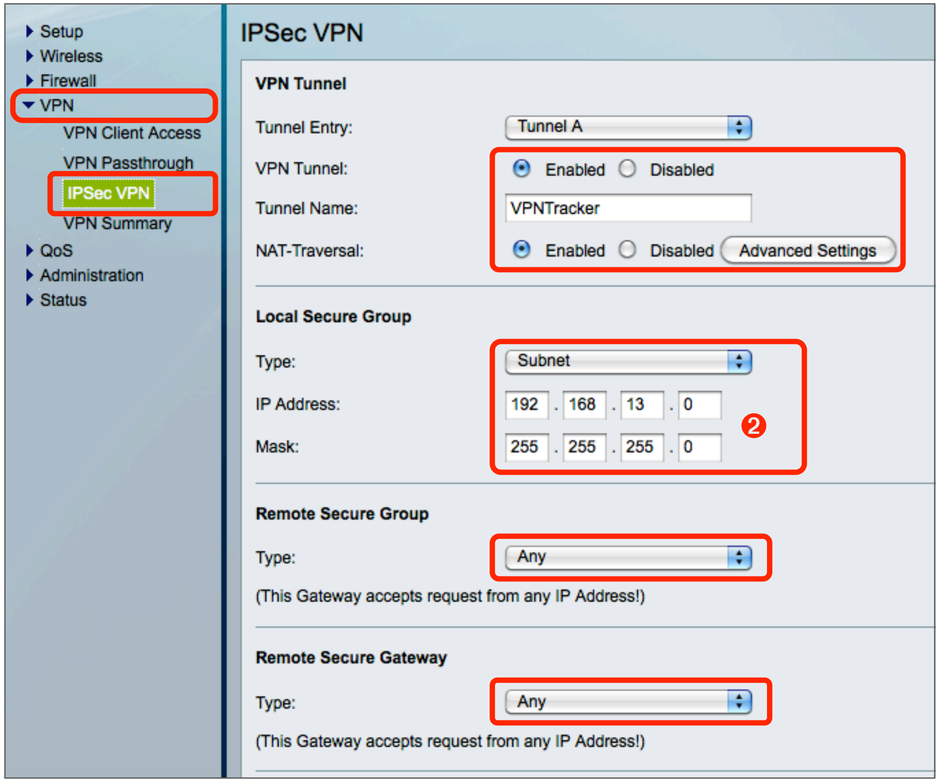
Subnet Mask: 255.255.255.0

- **Internet Connection**: Write down the **IP address** of your VPN gateway (here: 203.0.113.1) as ❶ on your → *Configuration Checklist*

  If you have a dynamic DNS (DynDNS) service set up for your router, you can write it down instead.

Step 2 – Set up VPN

- Go to **VPN** > **IPSec VPN**



IPSec VPN

VPN Tunnel

Tunnel Entry: Tunnel A

VPN Tunnel: ● Enabled ○ Disabled

Tunnel Name: VPNTracker

NAT-Traversal: ● Enabled ○ Disabled

Local Secure Group

Type: Subnet

IP Address: 192 . 168 . 13 . 0

Mask: 255 . 255 . 255 . 0

❷

Remote Secure Group

Type: Any

(This Gateway accepts request from any IP Address!)

Remote Secure Gateway

Type: Any

(This Gateway accepts request from any IP Address!)

VPN Tunnel

- **IPSec VPN Tunnel**: **Enable** the new VPN tunnel setting
- **Tunnel Name**: Enter a new VPN tunnel name (here: **VPNTracker**)

Local Secure Group

- **Type**: Choose **Subnet** from the pop-up
- **IP Address / Mask**: These should already be properly filled in by the device to match its LAN. Write them down as ❷ on your → *Configuration Checklist*

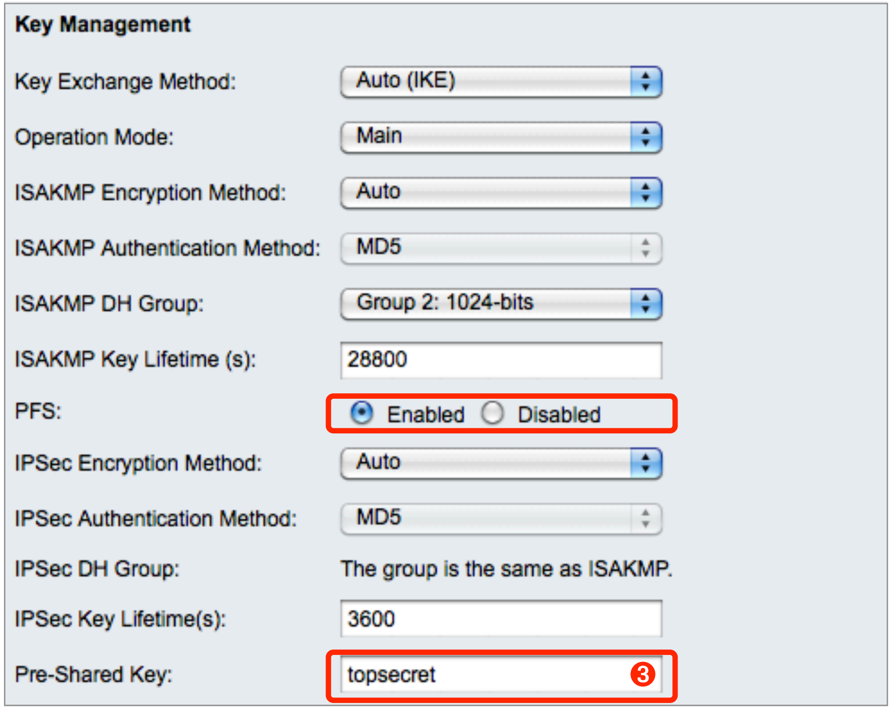
Remote Secure Group

- **Type**: Choose **Any** from the pop-up

Remote Secure Gateway

- **Type**: Choose **Any** from the pop-up

Key Management (Phase 1 / Phase 2)



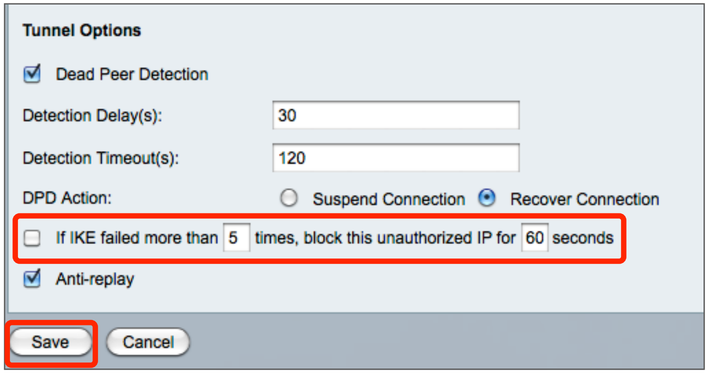
Key Management

Key Exchange Method:	Auto (IKE)
Operation Mode:	Main
ISAKMP Encryption Method:	Auto
ISAKMP Authentication Method:	MD5
ISAKMP DH Group:	Group 2: 1024-bits
ISAKMP Key Lifetime (s):	28800
PFS:	● Enabled ○ Disabled
IPSec Encryption Method:	Auto
IPSec Authentication Method:	MD5
IPSec DH Group:	The group is the same as ISAKMP.
IPSec Key Lifetime(s):	3600
Pre-Shared Key:	topsecret ❸

- **PFS**: Set PFS (Perfect Forward Secrecy) to **enabled**
- **Pre-Shared Key**: Enter a good password and write it down as ❸ on your → *Configuration Checklist*. This password will be needed to connect to this VPN connection
- Make sure the other settings on your device match those shown

We are using **Auto** for Phase 1 (ISAKMP) and Phase 2 (IPsec). The device will accept the encryption and authentication algorithms the client proposes. If you wish to **enforce specific algorithms** on the VPN gateway, please make sure to match these settings exactly in VPN Tracker (Advanced tab). **We strongly recommend setting up and testing the connection with Auto before making any changes..**

Tunnel Options



Tunnel Options

☑ Dead Peer Detection

Detection Delay(s):	30
Detection Timeout(s):	120
DPD Action:	○ Suspend Connection ● Recover Connection

□ If IKE failed more than 5 times, block this unauthorized IP for 60 seconds

☑ Anti-replay

- To prevent you from being locked out while setting up and testing the connection, it is very important to **disable** the checkbox „**If IKE failed more than … times, block this unauthorized IP for … seconds**"

If you wish, you can enable this checkbox again once you have completed setup and testing of this VPN connection.

- Click **Save** to complete the IPSec VPN setup

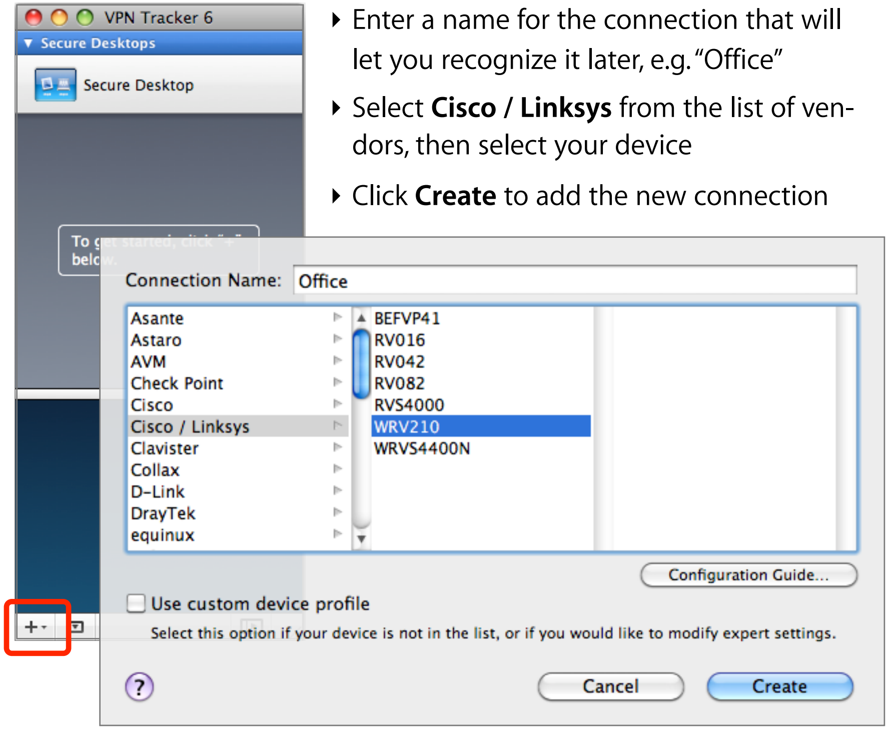
Task 2 – VPN Tracker Configuration

After finishing task 1, you should now have a completed → *Configuration Checklist* containing your VPN gateway's settings. We will now create a matching configuration in VPN Tracker.

Step 1 – Add a Connection

Open VPN Tracker, and click the plus button in the bottom left corner of the window to add a new connection:

- Enter a name for the connection that will let you recognize it later, e.g. "Office"
- Select **Cisco / Linksys** from the list of vendors, then select your device
- Click **Create** to add the new connection



Connection Name: Office

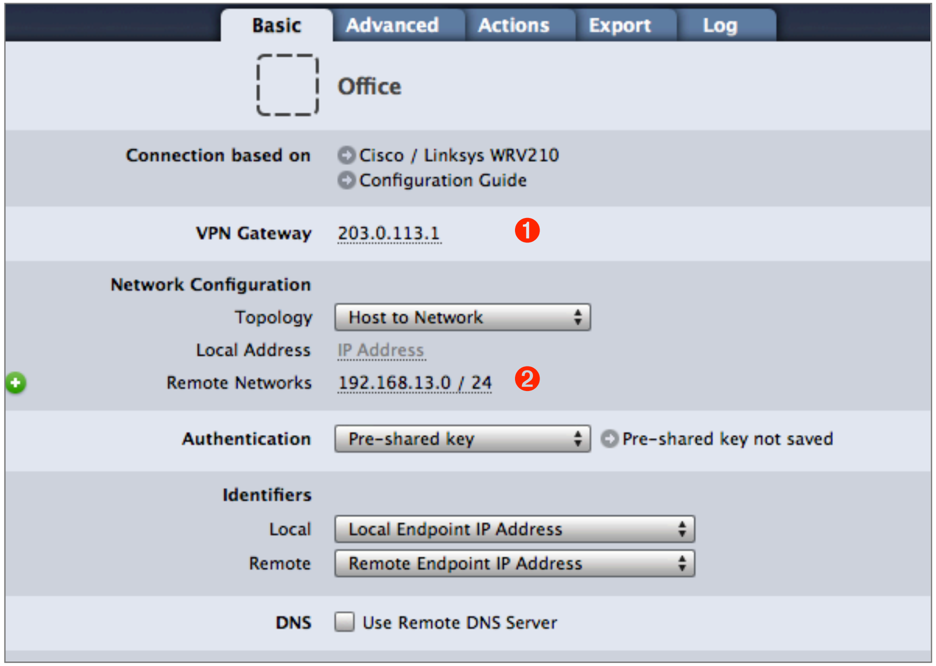
Cisco / Linksys → WRV210

□ Use custom device profile

Select this option if your device is not in the list, or if you would like to modify expert settings.

Step 2 – Configure the VPN Connection

Once you have added the new connection, there are a few settings that need to be customized to match what is configured on your VPN gateway.



Connection based on: Cisco / Linksys WRV210; Configuration Guide

VPN Gateway: 203.0.113.1 ❶

Network Configuration

Topology: Host to Network

Local Address: IP Address

Remote Networks: 192.168.13.0 / 24 ❷

Authentication: Pre-shared key — Pre-shared key not saved

Identifiers

Local: Local Endpoint IP Address

Remote: Remote Endpoint IP Address

DNS: □ Use Remote DNS Server

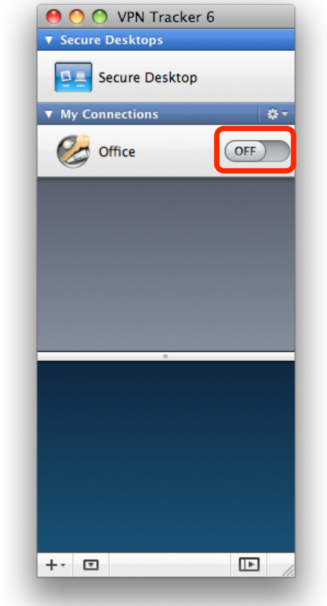
- **VPN Gateway**: Enter the WAN IP address of your VPN gateway you wrote down as ❶ from your → *Configuration Checklist*
- **Local Address**: Leave empty for now. Depending on your setup, you may have to set a specific local address later. Refer to → *Supporting Multiple Users* on when and how to set a specific local address.
- **Remote Networks**: Enter the network address of the network that is being accessed through the VPN tunnel ❷. Separate the subnet mask with a forward slash („/")

Step 3 – Test the VPN Connection

It ‘s time to go out!

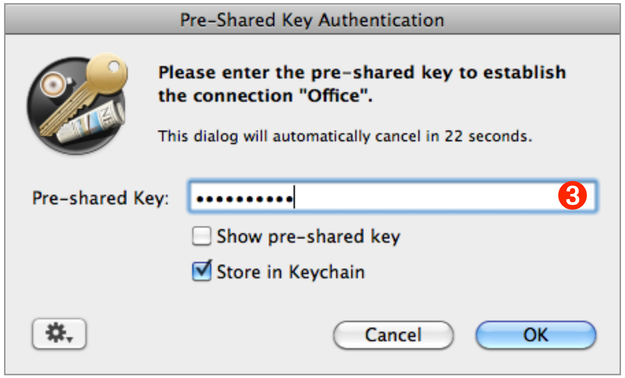
You will not be able to test and use your VPN connection from within the internal network that you want to connect to. To test your connection, you will need to connect from a different location. For example, if you are setting up a VPN connection to your office, test it from home. If you are setting up a VPN connection to your home network, test it from an Internet cafe, or go visit a friend.

Start your connection



- Connect to the Internet
- Make sure that your Internet connection is working – open your Internet browser and try to connect to http://www.equinux.com
- Open VPN Tracker if it’s not already running
- Slide the ON/OFF slider for the connection you have just configured to **ON**

When prompted for your pre-shared key:



Please enter the pre-shared key to establish the connection "Office".

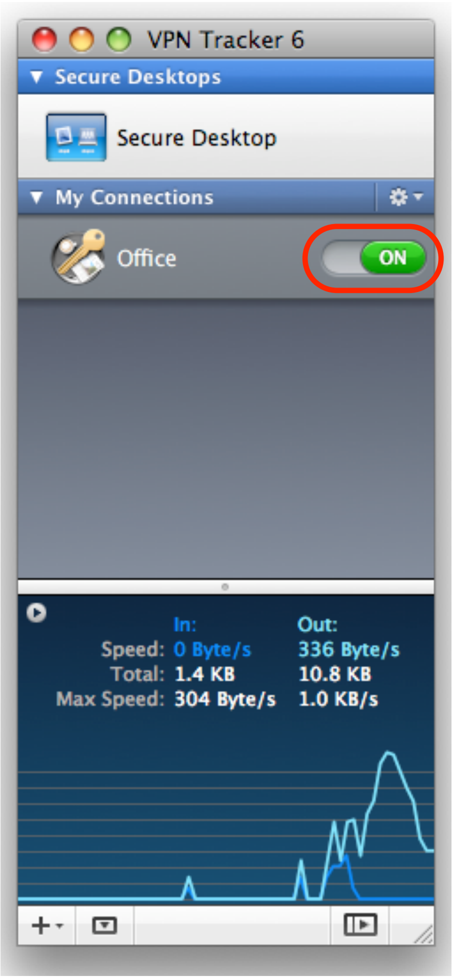
This dialog will automatically cancel in 22 seconds.

Pre-shared Key: ••••••••••

□ Show pre-shared key

☑ Store in Keychain

- **Pre-shared key**: Enter the pre-shared key that you configured on the VPN gateway ❸
- Optional: Check the box **Store in Keychain** to save the password in your keychain so you are not asked for it again when connecting the next time
- Click **OK**



```
            In:           Out:
    Speed:  0 Byte/s      336 Byte/s
    Total:  1.4 KB        10.8 KB
Max Speed:  304 Byte/s    1.0 KB/s
```

- If the slider goes back to **OFF** after starting the connection, or after entering your pre-shared key, please read the → *Troubleshooting* section of this document
- If the slider goes to **ON** and turns green after a while, you have successfully established a connection
- **Congratulations**!

Troubleshooting

In most cases, your connection should work fine if you follow the instructions above. If you cannot connect, please read on.

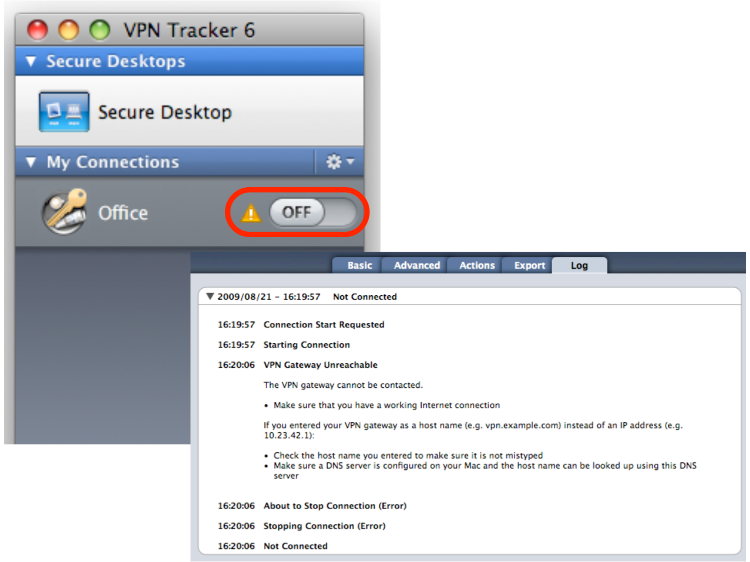
VPN Connection Fails to Establish

ON/OFF slider goes back to OFF right away

If the slider goes back to **OFF** right away, please make sure you have entered all the required information. VPN Tracker will highlight fields that are missing or obviously incorrect information.

ON/OFF slider goes back to OFF after a while

If the connection **ON**/**OFF** slider goes back to **OFF** a while after attempting to start the connection, please go to the **Log** tab to get more information about the issue (or click the warning triangle to be automatically taken to the **Log** tab). VPN Tracker will display detailed suggestions for a solution:



```
▼ 2009/08/21 – 16:19:57   Not Connected

16:19:57   Connection Start Requested

16:19:57   Starting Connection

16:20:06   VPN Gateway Unreachable

           The VPN gateway cannot be contacted.

           • Make sure that you have a working Internet connection

           If you entered your VPN gateway as a host name (e.g. vpn.example.com) instead of an IP address (e.g.
           10.23.42.1):

           • Check the host name you entered to make sure it is not mistyped
           • Make sure a DNS server is configured on your Mac and the host name can be looked up using this DNS
             server

16:20:06   About to Stop Connection (Error)

16:20:06   Stopping Connection (Error)

16:20:06   Not Connected
```

No Access to the Remote Network

If the connection slider goes to **ON** and turns green, but you cannot access resources (servers, email, etc.) through the VPN connection please check the following points.

Connect to an IP address (instead of a host name)

If you are using a host name (e.g. server.example.com) instead of an IP address (e.g. 192.168.13.42) to connect to a resource , please try using the resource's IP address instead. If the connection works when using the IP address, but not when using a host name, please make sure that your Mac's DNS server or the "Remote DNS" server that you have configured on your VPN gateway is able to resolve this host name to an IP address.

Test VPN Availability again

In many networks your Mac will be behind a router that performs Network Address Translation (NAT). For a VPN connection to be established through such a router, VPN Tracker can use different methods, but not all of them may be supported by your local router or your VPN gateway.

VPN Tracker automatically runs a test to detect the proper method for your particular Internet connection when you first connect using this Internet connection. However, test results could become outdated by changes to the local router, so it is a good idea to test again if there are problems.

- Select **Tools** > **Test VPN Availability** from the menu
- Click **Test Again** and wait until the test has completed
- Try connecting again

Check the Local Address setting

In order for replies to reach VPN Tracker, make sure that the **Local Address** (Basic tab) is empty, or, if you have a fixed address configured, that this address is **not** part of the remote network (see → *Supporting Multiple Users*).

Further Questions?

You can find the latest news and compatibility information on our support and FAQ website:

http://www.equinux.com/support

If you need to contact equinux Technical Support

If you can't resolve your issue with the information available on our website or in this guide and would like to contact Technical Support through our website, please be sure to include at least the following information:

- The manufacturer and model and firmware revision of the VPN gateway
- A Technical Support Report from VPN Tracker (Help > Generate Technical Support Report)
- Screenshots of what you have configured on your VPN gateway, in particular all VPN-related settings
- A description of the problem and the troubleshooting steps you have taken

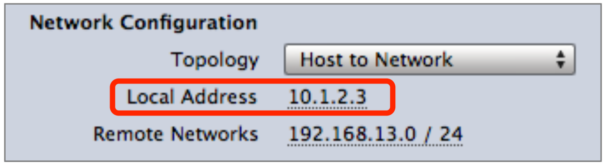
Supporting Multiple Users

Once your VPN expands to multiple users you must ensure that IP addresses do not conflict by assigning each user their own IP address.

Preventing IP Address Conflicts

How IP Addresses are Assigned to VPN Clients

The **Local Address** in VPN Tracker is the IP address that the Mac will be using in the remote network when connected through VPN.



Network Configuration
Topology: Host to Network
Local Address: 10.1.2.3
Remote Networks: 192.168.13.0 / 24

- If the Local Address field contains a **fixed address** this address is used. The address must be unique among all users of the VPN connection
- If the Local Address field is left **empty**, the Mac's actual local IP address (as shown in System Preferences > Network) is used.
  With multiple users, it's easily possible that two users end up with the same local IP address on their respective Macs (e.g. the private IP address 192.168.1.2). You will therefore have to **use a fixed address when multiple users connect to the VPN**

Step 1 – Choose the Local Addresses

Choose the local addresses for your VPN clients so that

- the local addresses are **not** part of the VPN's remote network (in most cases the VPN gateway's LAN)
- each client has its **own, unique** IP address

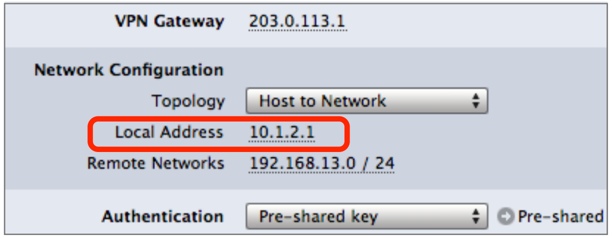
Example: The VPN gateway 's LAN in our example is the network 192.168.13.0/24 (= 192.168.13.0/255.255.255.0). For the local addresses, choose an arbitrary private network that is not part of this network, such as 10.1.2.0/24. For each user, pick a different IP address from that network to be used as the Local Address in VPN Tracker:

User	IP Address
Alice	10.1.2.1
Bob	10.1.2.2
Charlie	10.1.2.3
…	10.1.2...

Please refer to your VPN gateway's data-sheet for the maximum number of users that is supported.

⚠ The IP addresses may **not** be part of the remote network since your VPN gateway cannot act as an ARP proxy

Step 2 – Configure the Local Address in VPN Tracker



VPN Gateway: 203.0.113.1
Network Configuration
Topology: Host to Network
Local Address: 10.1.2.1
Remote Networks: 192.168.13.0 / 24
Authentication: Pre-shared key

- **Local Address**: Enter the IP address that you have chosen for this user (here: 10.1.2.1 for the user **Alice**)

⚠ If your VPN gateway is **not** the default gateway (router) of its network, you will have to ensure that traffic for the chosen IP addresses is routed back to the VPN gateway instead of to the usual default gateway (e.g. by adding a route on the default gateway to the VPN gateway for these IPs).