



VPN Configuration Guide

DrayTek Vigor / VigorPro



VPN Tracker 365

Remote Dial-In User Profile

equinix AG and equinix USA, Inc.

© 2015 equinix USA, Inc. All rights reserved.

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

The equinix logo is a trademark of equinix AG and equinix USA, Inc., registered in the U.S. and other countries.

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

www.equinix.com

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

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

Introduction	4
Important Prerequisites.....	5
Scenario.....	6
Terminology	7
My DrayTek Configuration	8
Task 1 – Configure your DrayTek	9
Step 2 - Add a New Remote Dial-In User	10
Step 3 - Configure the New Remote Dial-In User	11
Step 4 - Set the Pre-Shared Key	12
Step 5 - Retrieve the LAN Settings	13
Task 2 – Configure VPN Tracker	14
Step 1 – Add a VPN connection	14
Task 3 – Test the VPN Connection	16
It's time to go out!	16
Start your connection	16
Supporting Multiple Users	18
Preventing IP Address Conflicts.....	18
Configuring the DrayTek for Multiple Users	19
Configuring VPN Tracker for Multiple Users	19
Troubleshooting	20
Can't Connect to VPN.....	20
No Access to the Remote Network	21
Appendix	23
The Role of the Local Address in VPN Tracker	23

Introduction

This document describes how VPN Tracker can be used to establish a connection between a Mac running Mac OS X and a DrayTek Vigor/VigorPro firewall/router device.

Note This documentation is only a supplement to, not a replacement for, the instructions included with your DrayTek device. Please be sure to read those instructions and understand them before starting. The different DrayTek model / firmware revisions have different VPN capabilities. For definite information, please refer to your device's

VPN Gateway Configuration

The first part of this guide will show you how to configure a VPN tunnel on your DrayTek device.

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.

Troubleshooting and Advanced Topics

Troubleshooting tips can be found in the last part of this guide. There you can also find a chapter on supporting VPN connections for multiple users.

Tip If you are setting up VPN on your device for the first time, we strongly recommend you start out with the tutorial-style setup in the first and second part of this document.

Important Prerequisites

Your VPN Gateway

- ▶ This guide applies to DrayTek Vigor/VigorPro devices that have support for IPsec VPN Remote Dial-In User / Teleworker Profiles, these include
 - Vigor2110 Series
 - Vigor2200 Series¹
 - Vigor2700²/2710 Series
 - Vigor2800/2820 Series
 - Vigor2910/2930/2950 Series
 - Vigor3100 Series
 - VigorPro 5300/5500/5510 Series
- ▶ Make sure you have the newest available firmware installed on your device

Your Mac

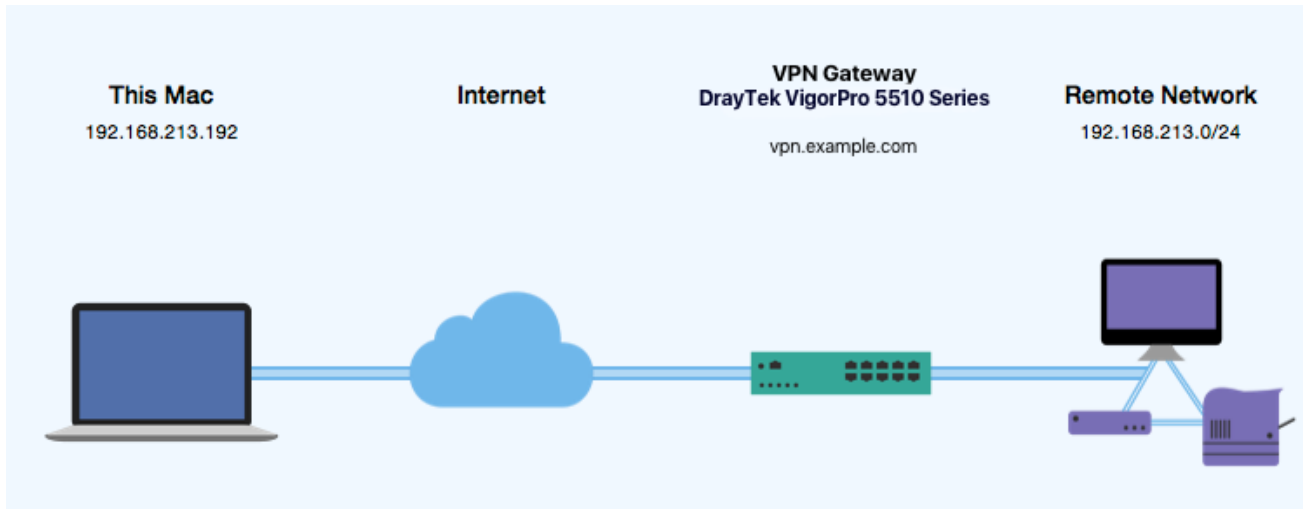
- ▶ VPN Tracker 365. Make sure you have all available updates installed. The latest VPN Tracker release can always be obtained from <http://www.vpntracker.com>

¹ Vigor2200V/VG only. Earlier devices use a different firmware that does not support IPsec VPN with Remote Dial-In User Profiles, please refer to the VPN Tracker 4 documentation available at <http://www.vpntracker.com/interop> for configuration instructions

² Vigor2700e/2700Ge have no IPsec VPN capabilities and are not supported

Scenario

In our example, we need to connect an employee's Mac to an office network. The following diagram illustrates this scenario:



This guide assumes that the Mac running VPN Tracker already has internet connectivity. The office's DrayTek 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 host name: `vpn.example.com`.

The VPN gateway has a second network interface which is connected to the internal office network (LAN). In our example, the office network has the IP range 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 DrayTek Configuration

TIP To set up your VPN connection, you'll need to keep track of certain pieces of information. Those details are indicated by red numbers. Throughout this guide we will be referencing those numbers.

① Peer ID: _____

② Pre-Shared Key: _____

③ LAN IP Address: _____ . _____ . _____ . _____

④ LAN Subnet Address: _____ . _____ . _____ . _____

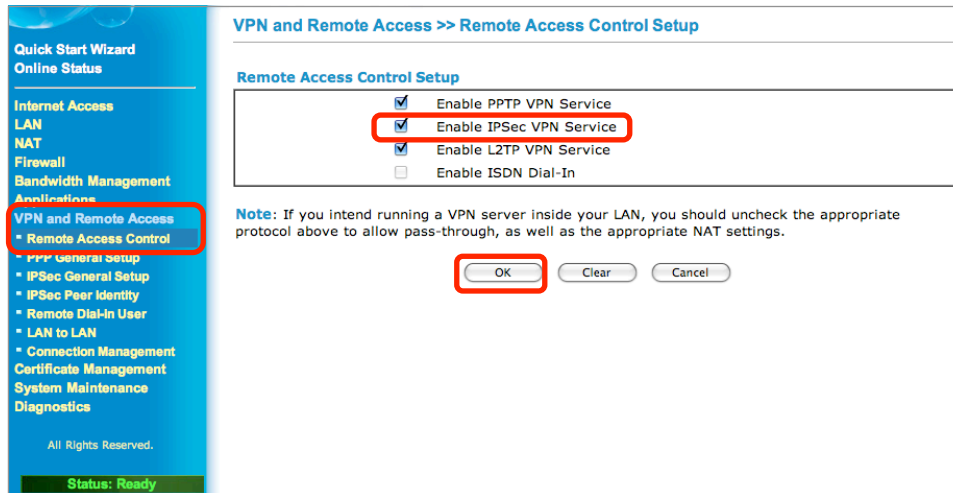
⑤ LAN Network Address: _____ . _____ . _____ . _____

⑥ WAN IP Address: _____ . _____ . _____ . _____ (or DNS host name _____)

Task 1 – Configure your DrayTek

This section describes the configuration of your DrayTek Vigor VPN router. If you do not yet have VPN configured and in use on your device, please proceed exactly as described in this section. We will be creating a connection using a Remote Dial-in User.

Step 1 – Enable the IPsec VPN Service



The screenshot shows the 'VPN and Remote Access >> Remote Access Control Setup' configuration page. On the left sidebar, 'VPN and Remote Access' is selected, and 'Remote Access Control' is highlighted. The main content area shows the 'Remote Access Control Setup' section with the following options:

- Enable PPTP VPN Service
- Enable IPsec VPN Service
- Enable L2TP VPN Service
- Enable ISDN Dial-In

A note below the options states: "Note: If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings." At the bottom of the configuration area, the 'OK' button is highlighted with a red box, along with 'Clear' and 'Cancel' buttons.

- ▶ Access your device's web configuration interface and enter your user name and password, if required
- ▶ Select "VPN and Remote Access"
- ▶ Click "Remote Access Control"
- ▶ Check the box "Enable IPsec VPN Service"
- ▶ Click "Ok"

Step 2 - Add a New Remote Dial-In User

The screenshot shows the 'VPN and Remote Access >> Remote Dial-in User' configuration page. On the left is a navigation menu with 'Remote Dial-In User' highlighted. The main area displays a table of 'Remote Access User Accounts' with columns for Index, User, and Status. The first row (Index 1) is highlighted with a red box. Below the table are navigation links and a status legend.

Index	User	Status	Index	User	Status
1.	???	x	9.	???	x
2.	???	x	10.	???	x
3.	???	x	11.	???	x
4.	???	x	12.	???	x
5.	???	x	13.	???	x
6.	???	x	14.	???	x
7.	???	x	15.	???	x
8.	???	x	16.	???	x

<< 1-16 | 17-32 >> [Next](#) >>

Status: v --- Active, x --- Inactive

- ▶ Click “Remote Dial-In User”
- ▶ Remote Access User Accounts: Click on an unused number (e.g. “1.”)

Step 3 - Configure the New Remote Dial-In User

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication

Enable this account
Idle Timeout second(s)

Allowed Dial-In Type

ISDN
 PPTP
 IPsec Tunnel
 L2TP with IPsec Policy
 SSL Tunnel / Microsoft® SSTP

Specify Remote Node
Remote Client IP or Peer ISDN Number

or Peer ID ❶

Netbios Naming Packet Pass Block
Multicast via VPN Pass Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)
SSL VPN
[Set SSL Web Proxy](#)

IKE Authentication Method

Pre-Shared Key
IKE Pre-Shared Key
 Digital Signature (X.509)

IPsec Security Method

Medium (AH)
 High (ESP)
 DES 3DES AES
Local ID (optional)

Callback Function

Check to enable Callback function
 Specify the callback number
Callback Number
 Check to enable Callback Budget Control
Callback Budget minute(s)

OK Clear Cancel

▶ User Accounts and Authentication

- ▶ Check the box “**Enable this account**”
- ▶ Make sure the **Idle Timeout** is set to “0” seconds

▶ Allowed Dial-In Type

- ▶ Check the box “IPsec Tunnel”
- ▶ If you don’t plan to be using the other options (e.g. PPTP), uncheck them

▶ Check the box “**Specify Remote Node**”

- ▶ **Peer ID**: Enter an identifier for this connection (e.g. “vpntracker”) ❶

▶ IKE Authentication Method

- ▶ Check the box “Pre-Shared Key”

▶ IPsec Security Method

- ▶ Uncheck the box “**Medium (AH)**”
- ▶ **High (ESP)**: We recommend checking 3DES and AES, but not DES. Make sure at least one method is always checked.

Note The peer ID is case-sensitive. Make sure to write down the peer ID, including capitalization.

Step 4 - Set the Pre-Shared Key

The screenshot shows the 'IKE Authentication Method' configuration in the Router Web Configurator. The 'Pre-Shared Key' option is selected, and the 'IKE Pre-Shared Key' button is highlighted. A pop-up window titled 'Router Web Configurator' shows the 'Pre-Shared Key' and 'Re-type Pre-Shared Key' fields, both with red question marks, and a 'Confirm' button highlighted.

- ▶ Click the “**IKE Pre-Shared Key**” button
- ▶ **Pre-Shared Key**: Enter a password for the connection **?**
- ▶ **Re-type Pre-Shared Key**: Enter the same password again **?**
- ▶ Click “**Confirm**” in the pop up window
- ▶ Click “**Ok**” to save the new Remote Dial-in User.

Step 5 - Retrieve the LAN Settings



System	
CPU Usage	: 8 %
Total Memory	: 16M
Memory usage	: 29 %

LAN	
MAC Address	: [REDACTED]
1st IP Address	: 192.168.13.1 3
1st Subnet Mask	: 255.255.255.0 4
DHCP Server	: No
Primary DNS	:
Secondary DNS	:

WAN 1 (InteropWAN)	
Link Status	: Connected
MAC Address	: [REDACTED]
Connection	: Static IP
IP Address	: 194.145.236.2 6
Default Gateway	: 194.145.236.1
Primary DNS	: 194.145.236.1
Secondary DNS	:

- ▶ Click on the large “**Vigor ... Series**” logo at the very top left corner of the configuration interface to get to the “**System Status**” display

▶ LAN IP Network Configuration

- ▶ Write down the “1st IP Address” **3**
- ▶ Write down the “1st Subnet Mask” **4**
- ▶ Calculate your **LAN Network Address** by applying the **LAN Subnet Mask 4** to the **LAN IP Address 3**:
 - ▶ Applying the subnet mask means setting those elements of the IP address to 0 where the subnet mask is 0, and preserving all elements where the subnet mask is 255. In our example:

LAN Subnet Mask	255 . 255 . 255 . 0
<i>applied to</i>	↓ ↓ ↓ ↓
LAN IP Address	192 . 168 . 13 . 1

LAN Network Address 192 . 168 . 13 . 0

Write down the **LAN Network Address** you have calculated as **5**

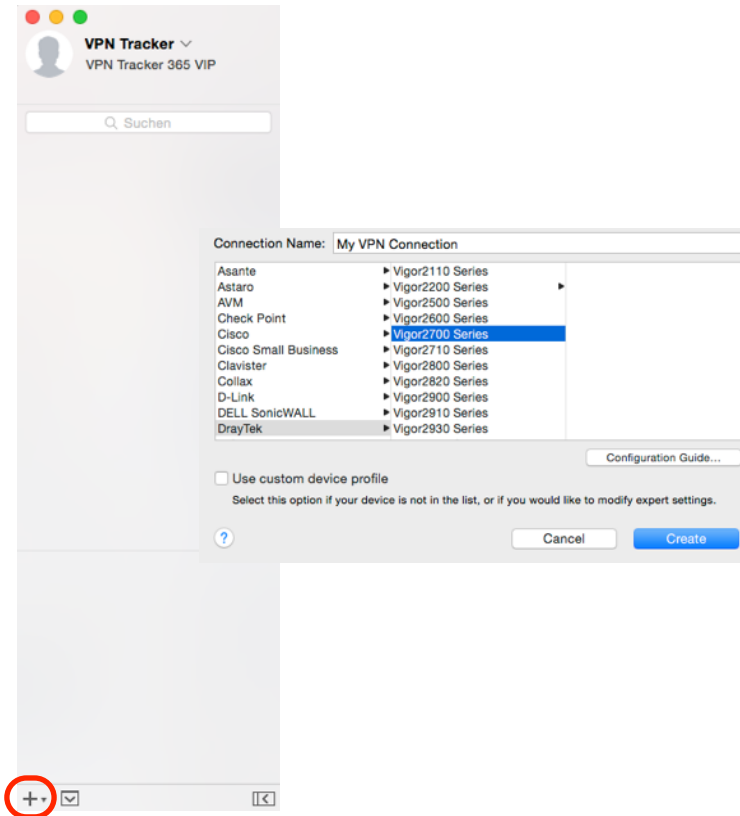
▶ WAN IP Network Configuration

- ▶ Write down the IP address **6**

Task 2 – Configure VPN Tracker

This section describes how to configure VPN Tracker to connect to your DrayTek. You will need the configuration information you collected during Task 1.

Step 1 – Add a VPN connection



- ▶ Start VPN Tracker
- ▶ Click the “+” button in the main window

You will be asked to select a device profile for the new connection:

- ▶ Select “**DrayTek**” from the list
- ▶ Select your device from the list of DrayTek devices.
 - ▶ If there is more than one choice, choose “Remote Dial-In User Profile”.

Do **not** choose the legacy “LAN-to-LAN” profile if your device supports IPsec VPN for Remote Dial-In User profiles (the LAN-to-LAN profile configuration is not described in this guide).

- ▶ **Connection Name:** Choose a name for your connection (e.g. “Office”)
- ▶ Click “OK”

Step 2 – Configure the VPN Connection

The screenshot shows the 'Basic' tab of a VPN configuration page. The interface is divided into several sections:

- Connection Name:** My VPN Connection. Below it, 'Connection based on' is set to 'DrayTek Vigor2700 Series' with a link to the 'Configuration Guide'.
- VPN Gateway:** Host Name or IP Address. A red circle with the number 6 is next to the input field.
- Network Configuration:**
 - Topology:** Host to Network (dropdown menu).
 - Local Address:** IP Address (input field with a help icon).
 - Remote Networks:** Network Address (input field with a red circle and number 4). A red circle with the number 5 is next to the 'Remote Networks' label.
- Authentication:** Pre-shared key (dropdown menu) with the text 'Pre-shared key not saved'.
- Identifiers:**
 - Local:** Fully Qualified Domain Name (FQDN) (dropdown menu) with 'Peer ID' (input field with a red circle and number 1).
 - Remote:** Remote Endpoint IP Address (dropdown menu).
- DNS:** Use Remote DNS Server (checkbox, currently unchecked).

- ▶ **VPN Gateway:** Enter your DrayTek's public IP address 6. If you are using Dynamic DNS, or if the device has a DNS host name, use it instead (in our example, we are using the host name "vpn.example.com")
- ▶ **Local Address:** Can be left empty for now. You may have to eventually enter a specific IP address here, please see the chapter on "Supporting Multiple Users" for details
- ▶ **Remote Networks:** Enter the calculated network address 5 and the subnet mask 4 of the network that is being accessed through the VPN tunnel. Separate the subnet mask with a forward slash ("/")
- ▶ **Local Identifier:** Enter the **Peer ID** from your DrayTek (e.g. "vpntracker") 1

Note If you are missing any of the required information, refer back to the previous chapter.

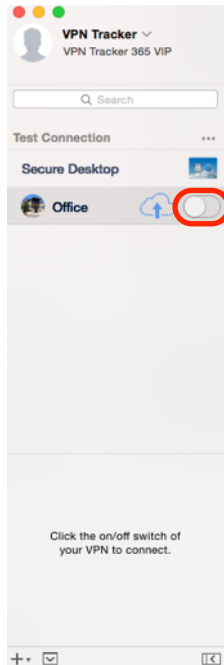
Task 3 – Test the VPN Connection

This section explains how to start and test your 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. In order 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

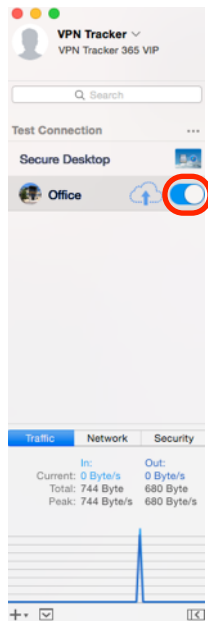


- ▶ Connect to the Internet
- ▶ Make sure that your Internet connection is working – open your Internet browser and try to connect to <http://www.equinux.com>
- ▶ Start VPN Tracker if it's not already running
- ▶ Slide the On/Off slider for the connection you have just configured to **On**

When you are prompted for your pre-shared key:



- ▶ **Pre-shared key:** Enter the pre-shared key that you configured on the VPN gateway 2
- ▶ Optionally, 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”



- ▶ 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!

Supporting Multiple Users

Once your VPN expands to multiple users (or even just yourself connecting from multiple computers simultaneously), there are certain issues you will have to consider. Primarily, you must ensure that IP addresses do not conflict. In addition to purely technical considerations, VPN Tracker makes it easy to distribute pre-configured connections to your users, and prevent the modification of VPN connections and access to confidential data.

Preventing IP Address Conflicts

If multiple users connect to your DrayTek at the same time, **you must ensure that each of them uses a different Local Address in VPN Tracker** by setting an individual Local Address for each of them.

Advanced Users A more detailed description of the Local Address setting is available in the last chapter of this

Choosing the Local Address

The Local Address must **not** be part of the remote network (i.e. the DrayTek's LAN) and the **same Local Address may not be used by two VPN clients** at the same time.

Example: The DrayTek's LAN in this example is the network 192.168.13.0/24 (= 192.168.13.0/255.255.255.0). Choose an arbitrary [private network](#) that is not part of this network, such as 10.22.13.0/24, and manually assign each user of the VPN a different IP address from that network to be used as the Local Address in VPN Tracker.

User	IP Address
alice	10.22.13.1
bob	10.22.13.2
charlie	10.22.13.3
...	10.22.13._

Configuring the DrayTek for Multiple Users

Adding new VPN users to your DrayTek is easy: For each additional VPN user, simply add a new “Remote Dial-In User” profile, with a different Peer ID, and – if desired – a different pre-shared key. With some DrayTek models and firmware revisions it may be possible for multiple users to share a single Remote Dial-In User Profile. However, it will still be necessary for each of the users of such a shared profile to have a different “Local Address” in VPN Tracker.

Note The total number of VPN users, as well as the number of VPN users that can be connected concurrently, is limited by your DrayTek’s firmware and hardware. Please refer to your device’s data sheet for details.

Configuring VPN Tracker for Multiple Users

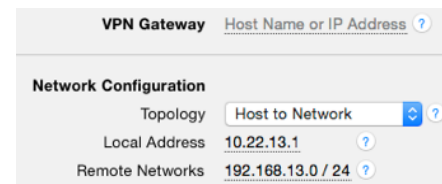
When adding additional VPN users to your DrayTek for the first time, edit the VPN Tracker connection of the original user to use the fixed “Local Address” you have chosen for the user.

Once the initial user’s connection has been modified, you can begin to set up the VPN Tracker connections for other users. The setup is mostly identical to the first user’s connection, with the following differences:

- ▶ The “Local Address” must be set to the IP address chosen for this particular user
- ▶ The “Local Identifier” must be set to the Peer ID of the user’s Remote Dial-In Profile on the DrayTek

Note Some DrayTek models (in particular those that do not support NAT-Traversal) only accept a single VPN connection from a particular public IP address. With these devices, it will not be possible to connect two computers from behind the same NAT router to the VPN.

- ▶ If you are using a different pre-shared key for this user’s Remote Dial-In Profile, use this pre-shared key



The screenshot shows a configuration page for a VPN Gateway. At the top, there is a field for 'Host Name or IP Address' with a question mark icon. Below this is a section titled 'Network Configuration'. Inside this section, there are three rows of settings: 'Topology' is set to 'Host to Network' with a dropdown arrow and a question mark; 'Local Address' is set to '10.22.13.1' with a question mark; and 'Remote Networks' is set to '192.168.13.0 / 24' with a question mark.

Troubleshooting

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

Can't Connect to VPN

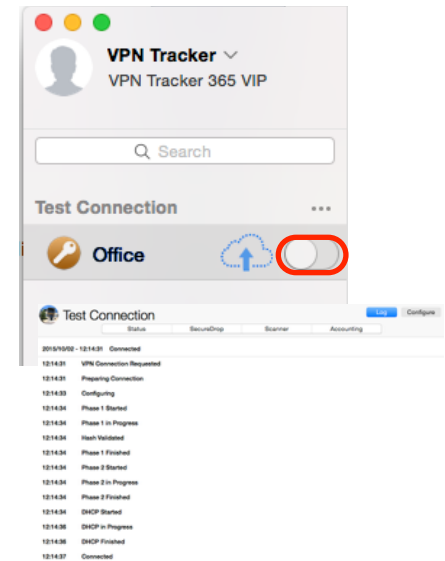
On/Off Slider goes back to “Off” right away

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 error (or click the warning triangle to be automatically taken to the “Log” tab).

Depending on the actual problem, VPN Tracker will display detailed suggestions for a solution.



No Access to the Remote Network

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

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

If you are not connecting to the resource by IP address (e.g. 192.168.1.42), but are using a host name (e.g. server.example.com), 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 in VPN Tracker 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 that the IP address you are connecting to is part of the VPN's remote network

Check that the IP address you are connecting to is actually part of the remote network(s). Also double-check the network mask that you have configured for the remote network(s) in VPN Tracker.

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 settings
- ▶ A detailed description of the problem and the troubleshooting steps you have taken

Appendix

The Role of the Local Address in VPN Tracker

The local address is the IP address that your Mac uses in the remote network when connected through VPN. If the Local Address field is left empty, the Mac's actual local IP address (as shown in System Preferences > Network) is used

Advanced Users The Local Address is used as the endpoint of the IPsec Security Association (SA) on the VPN Tracker side that is established in phase 2 of the connection process.

When to Set the Local Address in VPN Tracker

Always use a fixed Local Address if

- ▶ multiple clients (users/computers) use the VPN
- ▶ the DrayTek device is not the default gateway (router) in the remote network

Choosing the Local Address

When connecting to a DrayTek device, the Local Address **must not be part of the remote network** (i.e. the DrayTek's LAN) and the **same Local Address may not be used by two VPN clients** at the same time. If there is only a single user of the VPN, this will often automatically be the case if the Local Address field is simply left empty, and VPN Tracker therefore uses the Macs local IP address. However, in all other circumstances, you should configure a specific address.

Example: The DrayTek's LAN in this example is the network 192.168.13.0/24 (= 192.168.13.0/255.255.255.0). Choose an arbitrary [private network](#) that is not part of this network, such as 10.22.13.0/24, and manually assign each user of the VPN a different IP address from that network to be used as the Local Address in VPN Tracker.

User	IP Address
alice	10.22.13.1
bob	10.22.13.2
charlie	10.22.13.3
...	10.22.13._

Local Addresses for the More Curious

Why can't I use a Local Address from my DrayTek's LAN?

It may sound a bit unusual to use IP addresses that are not part of the DrayTek's LAN. The reason for this is that the DrayTek cannot act as a so-called "ARP Proxy" for its VPN clients. Computers on the DrayTek's LAN therefore must be "tricked" into sending replies for VPN clients to the DrayTek by using IPs from outside the local network (for which replies are sent to the default gateway).

My users connect from different places, from different IPs. Why do I still need to give them different Local Addresses?

In most cases, the connecting Macs will be behind routers (DSL routers, wireless access points, ...) that perform Network Address Translation (NAT), meaning they map several private IP addresses onto a single public IP address. The Macs themselves will have a private IP address for their Ethernet or AirPort interface, and this is the IP address that is used by VPN Tracker if the Local Address field is empty.

Because of this, the likelihood of two Macs using the same local address is very high: Many NAT routers are by default configured to use the same private networks (192.168.1.0/24 and 10.0.0.0/24 are popular), and therefore there is a good chance that two clients connecting from entirely different places will have the same local IP address assigned by their respective local router. Therefore it is essential to configure a different Local Address in VPN Tracker for each VPN user if multiple users connect concurrently.

Why do I need a fixed Local Address when my DrayTek is not the default gateway/router in its LAN?

If the DrayTek is not the default gateway, this means that computers the VPN clients communicate with do not connect to the Internet through the DrayTek.

In such an environment, you will have to ensure that those computers (and all other resources accessed through the VPN, such as printers and NAS drives) know where to send replies for VPN clients. This is much easier, if you know what IP

addresses your VPN clients will be using, and therefore you should enter an individual fixed IP address in the Local Address field on each VPN client.

Once you have decided on a range of IP address to be used for VPN clients, you can either

- ▶ set a route to the DrayTek for the VPN clients' IP addresses on each host that needs to communicate with VPN clients,
or
- ▶ have the default gateway redirect all traffic for the VPN clients' IP addresses to the DrayTek