



VPN Configuration Guide

Netgear FVS338 / FVX538 / FVS124G

Revision 1.0.1

equinux AG and equinux USA, Inc.

© 2006 equinux 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 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.

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

Created using Apple Pages.

www.equinux.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.

Finder and Mail are trademarks of Apple Computer, Inc. AppleCare is a service mark of Apple Computer, Inc., registered in the U.S. and other countries.

FileMaker is a trademark of FileMaker, Inc.

equinux 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 equinux has been advised of the possibility of such damages.

Introduction.....	5
Prerequisites.....	6
Scenario.....	7
Task 1 – Configure your Netgear router.....	9
Step 1 - Create a new IKE Policy.....	10
Step 2 - Create a new VPN Policy.....	11
Task 2 – Configure VPN Tracker.....	12
Step 1 - Create a new Connection.....	12
Step 3 - Network Settings.....	14
Step 4 - Authentication Settings.....	15
Step 5 - Identifiers Settings.....	16
Task 3 - Check the VPN connection.....	17
It's time to go out!.....	17
Test your connection.....	17
Troubleshooting.....	19
What's next?.....	20
Introduction.....	20
Known Limitations.....	20
Accessing Files.....	21
Accessing a FileMaker Database.....	23
Acquire more Licenses.....	27

Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a Netgear VPN router.

The Netgear gateway is configured as a router connecting a company LAN to the Internet.

This paper is only a supplement to, not a replacement for, the instructions that have been included with your Netgear. Please be sure to read those instructions and understand them before starting.

EQUINIX SHALL HAVE ABSOLUTELY NO LIABILITY FOR ANY DIRECT OR INDIRECT, SPECIAL OR OTHER CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE USE OF THE HOW-TO 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.

Prerequisites

First you have to make sure to use a recent Netgear firmware version. The latest release for your Netgear firewall can be obtained from <http://www.netgear.com/>

For the Netgear FVS124G Router, firmware version 1.1.33 has been used.

For the Netgear FVS338/FVX538 devices, firmware version 1.6.48 has been used.

Please note: Firmware versions prior to 1.6.48 are having some issues in conjunction with VPN Tracker. According to the Netgear support pages, you should restore the factory defaults, when upgrading from a previous firmware version with this model.

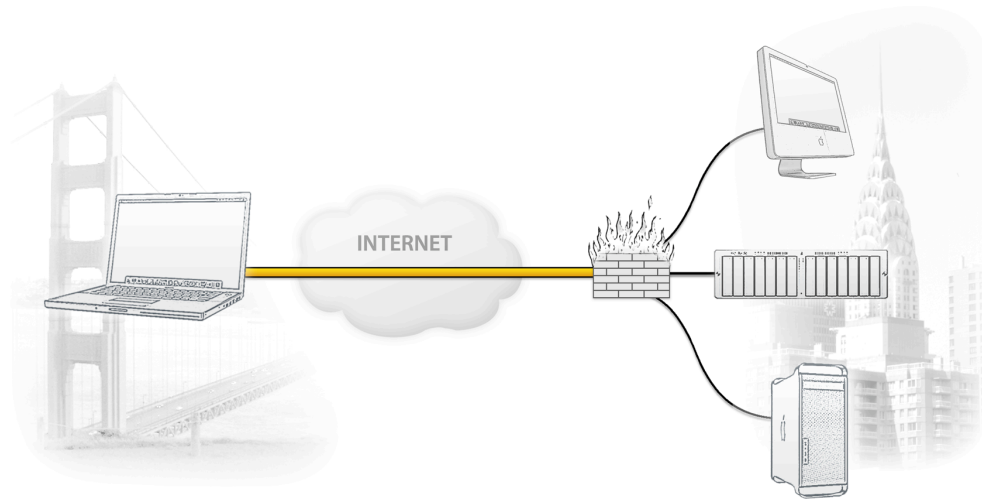
Please note: VPN Tracker has been only been tested with the Netgear and the above firmware version.

You will need one VPN Tracker Personal Edition license for each Mac connecting to the Netgear router.

We recommend one VPN Tracker Professional Edition for the administrator's Mac in order to export configuration files to the clients. VPN Tracker is compatible with Mac OS X version 10.2.5+, 10.3 and 10.4.1+

Scenario

In our example, we need to connect an employee's Mac Book in San Francisco to an office in New York. The following diagram illustrates this scenario:



The MacBook is directly connected to the Internet and has a public IP address, assigned by an ISP.

The office's VPN gateway is also connected to the Internet and can be accessed via an static IP address. The VPN gateway also has a second interface which is connected to the internal office network. In our example, the office network has the IP range 192.168.1.0/24.

A VPN tunnel will be established between the public interfaces in San Francisco and New York. Once the VPN tunnel is up, San Francisco can access the office network behind the VPN gateway.

Please note that the connection from a MacBook at home to an office network is just one possible scenario. The instructions also apply to connections from a desktop computer or notebook in your office to a VPN gateway at home or at another office. Please adapt the term "office network", which is used throughout this manual, to your scenario.

Task 1 – Configure your Netgear router

This section describes the configuration of your Netgear VPN router.

TIP When setting up a VPN, you'll have to handle a couple of parameters. Those parameters are marked with red dots with little numbers in it. Throughout the setup we will point back to those parameters.

Step 1 - Create a new IKE Policy

NETGEAR ProSafe VPN Firewall FX538 settings

IKE Policy Configuration

General
 Policy Name: vpntracker
 Direction/Type: Responder
 Exchange Mode: Aggressive Mode

Local
 Select Local Gateway: WAN 1 ☐ WAN 2 ☐
 Local Identity Type: Fully Qualified Domain Name **1**
 Local Identity Data: netgear.local

Remote
 Remote Host Configuration Record: None
 Remote Identity Type: Fully Qualified Domain Name **2**
 Remote Identity Data: vpntracker.local

IKE SA Parameters
 Encryption Algorithm: 3DES
 Authentication Algorithm: SHA-1
 Authentication Method: Pre-shared Key **3** (secretkey)
 Diffie-Hellman (DH) Group: Group 2 (1024 bit)
 SA Life Time: 3600 (secs)

X AUTHENTICATION
☐ IPSec Host ☐ Edge Device ☒ None

IKE Policy Configuration Help
 IKE provides automatic management of the Keys used in IPSec, and is used for "Auto" IPSec VPN policies. This screen is used to create or edit an IKE Policy.
General
 This section has general information about this IKE policy.
Policy Name - Enter an appropriate name to help you manage the IKE policies. This name is also used by remote VPN clients as part of the identity string in making client connections to the router.
Direction/Type - This setting is used when determining if the IKE policy matches the current traffic. Select the desired option.
 • Initiator - Outgoing connections are allowed, but incoming connections will be blocked.
 • Responder - Incoming connections are allowed, but outgoing connections will be blocked.
 • Both Directions - Both incoming and outgoing connections are allowed.
Exchange Mode - Options are "Main Mode" and "Aggressive Mode".
 • Main Mode is slower but more secure.
 • Aggressive mode is faster but less secure.
 • This setting must match the setting used on the remote VPN endpoint. Not all VPN endpoints support both modes.
Local
 Local Identity is used to identify this device to the remote VPN endpoint.
Local Identity Type
 Select the desired option to match the "Remote Identity Type" setting on the remote VPN endpoint.
 • WAN IP Address - your Internet IP address.
 • Fully Qualified Domain Name - your domain name.
 • Fully Qualified User Name - your name, E-mail address, or other ID.
 • DER ASN.1 DN - the binary DER encoding of your ASN.1 X.500 Distinguished Name.

- **Policy Name:** Enter an arbitrary name (e.g. vpntracker)
- **Direction/Type:** Select Responder
- **Exchange Mode:** Select Aggressive Mode
- **Local Identity Type:** Select Fully Qualified Domain Name
- **Local Identity Data:** Enter an arbitrary identifier (e.g. netgear.local) **1**
- **Remote Identity Type:** Select Fully Qualified Domain Name
- **Remote Identity Data:** Enter an arbitrary identifier (e.g. vpntracker.local) **2**
- **Pre-shared Key:** Enter an arbitrary key (e.g secretkey) **3**

Step 2 - Create a new VPN Policy

NETGEAR ProSafe VPN Firewall FVX538 settings

VPN - Auto Policy

General

Policy Name:

IKE policy:

Remote VPN Endpoint

Address Type:

Address Data:

SA Life Time: (Seconds)

(Kbytes)

PFS Key Group:

☐ IPsec PFS

Traffic Selector

Local IP

Subnet address:

Start IP address:

Finish IP address:

Subnet Mask:

Remote IP

Single address:

Start IP address:

Finish IP address:

Subnet Mask:

AH Configuration

☐ Enable Authentication

Authentication Algorithm:

ESP Configuration

☒ Enable Encryption

Encryption Algorithm:

☒ Enable Authentication

Authentication Algorithm:

☐ NETBIOS Enable

VPN Auto Policy Help

This screen allows you to define or edit an "Auto" VPN policy.

An "Auto" VPN policy uses the IKE (Internet Key Protocol) to exchange and negotiate parameters for the IPsec SA (Security Association). Because of this negotiation, it is not necessary for all settings on this VPN Gateway to match the settings on the remote VPN endpoint. Where settings must match, this is indicated.

General

These settings identify this policy and determine its major characteristics.

Name

Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.

IKE policy

The existing IKE policies are presented in a drop-down list.

The required IKE policy must be created BEFORE the VPN policy.

Select the desired IKE policy.

IKE Keep Alive

Enable this to ensure a VPN tunnel is re-established quickly if the connection is lost. If enabled, you must enter the Ping IP Address.

This address will be "pinged" to test the connection; it must be associated with the remote endpoint. Either the WAN or a LAN address can be used; a LAN address is preferable.

Remote VPN Endpoint

Select the desired option (IP address or Domain Name) and enter the address of the remote VPN Gateway/Server or client you wish to connect to.

Note: The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".

SA Life Time

This determines the time interval before the SA (Security Association) expires. (It will automatically be re-established if necessary.) While using a short time

- **Policy Name:** Enter an arbitrary name (e.g. vpntracker)
- **IKE policy:** Select your previously created IKE policy (e.g. vpntracker)
- **Remote VPN Endpoint:**
 - **Address Type:** Select IP Address
 - **Address Data:** Enter 0.0.0.0
- **Local IP:** Subnet address
- **Start IP address:** Enter the network address of the Netgear LAN (e.g. 192.168.1.0)
- **Subnet Mask:** Enter 255.255.255.0
- **Remote IP:** Select Single address
- **Start IP address:** Enter a virtual IP address for the VPN Tracker client (e.g. 10.1.2.3)
- **ESP Configuration -> Enable Encryption:** 3DES
- **ESP Configuration -> Enable Authentication:** SHA1

Task 2 – Configure VPN Tracker

This section describes the configuration of VPN Tracker for your Netgear router.

Step 1 - Create a new Connection

► Click on “New” in the VPN Tracker main window.



Step 2 - Connection Settings



- ▶ Select the vendor (**Netgear**)
- ▶ Select your VPN router model (e.g. **Netgear FVX538**)
- ▶ Make sure to enable "Initiate connection from this end"

TIP The pre-defined VPN Tracker connection for the Netgear router is based on the default settings for your Netgear VPN router. If you or the administrator changed any of the settings while configuring the device, you might have to adjust the connection type in VPN Tracker by double-clicking the model.

Step 3 - Network Settings

Connection: New York

Connection: New York

Topology: Host to Network

Network Port: Automatic

VPN Gateway Address: 169.1.2.3

Local Address: 10.1.2.3 optional 5

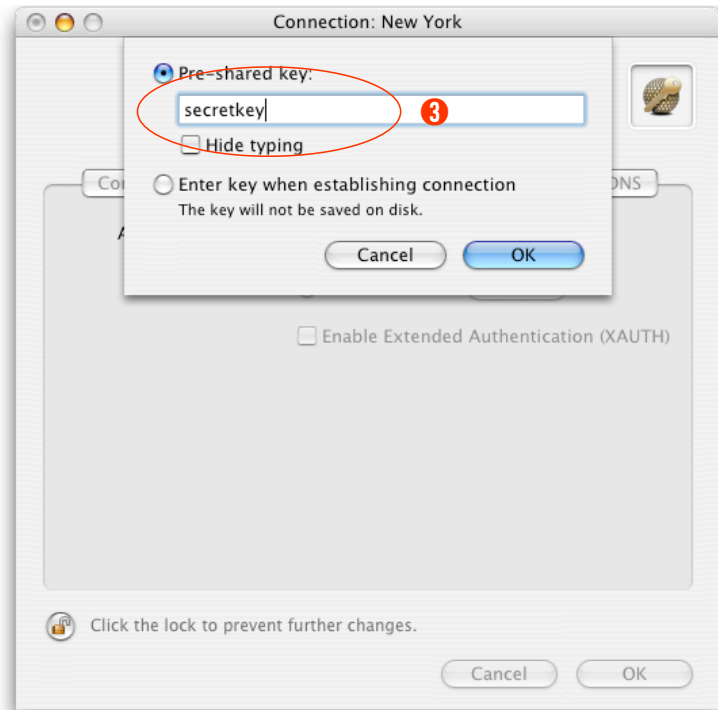
Remote Network/Mask: 192.168.1.0 / 255.255.255.0 4

Click the lock to prevent further changes.

Cancel OK

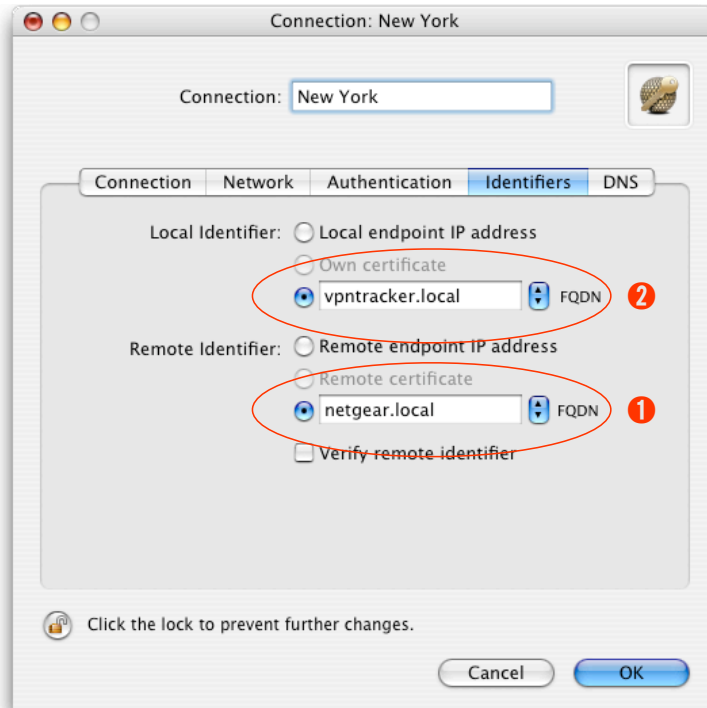
- ▶ **VPN Server Address:** Enter the public IP address of your VPN Gateway (e.g. 169.1.2.3)
- ▶ **Local Address:** Enter the virtual IP address you've chosen for the VPN Tracker client (e.g. 10.1.2.3) 5
- ▶ **Remote Network/Mask:** Enter network address and netmask of your office (Netgear) network. 4

Step 4 - Authentication Settings



- **Pre-shared key:** Enter the Pre-shared key you've used earlier when configuring the Netgear router. **3**

Step 5 - Identifiers Settings



- ▶ **Local Identifier:** Enter the remote identity data you've used when configuring the Netgear. (e.g. `vpntracker.local`) **2**
- ▶ **Remote Identifier:** Enter the local identity data you've used when configuring the Netgear. (e.g. `netgear.local`) **1**

TIP Please note, that the identifiers are switched in the VPN Tracker configuration. The local identifier in VPN Tracker corresponds to the remote identity data on your Netgear router and vice versa.

Task 3 - Check the VPN connection

This section explains how to start and test your VPN connection.

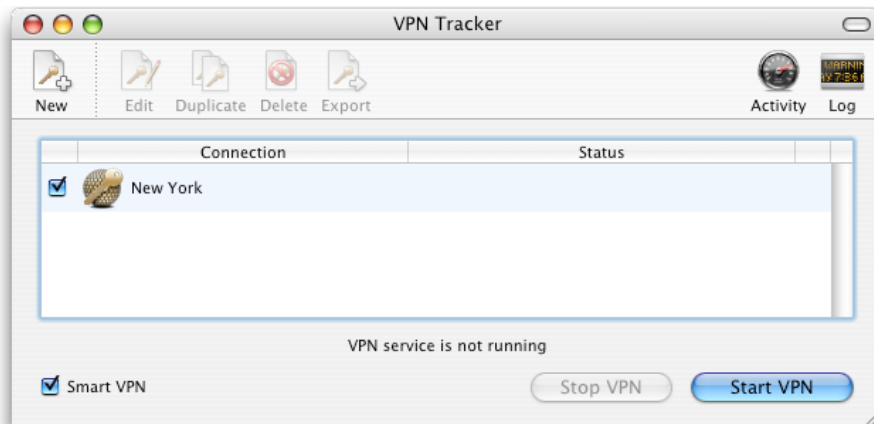
It's time to go out!

You will not be able to test and use your VPN connection from within your office network. In order to test your connection, you'll need to connect from a different location. That's why it's now time to go out. Take your MacBook Pro and have a coffee at your favorite Internet cafe or go visit a friend.

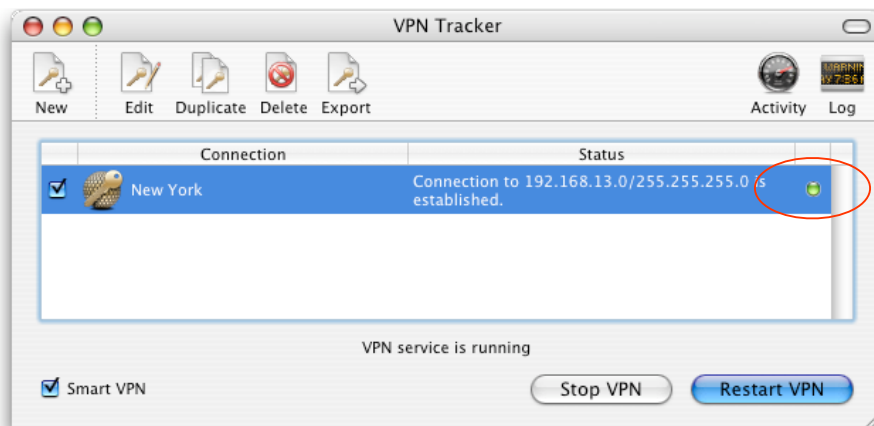
Test your connection

To test if everything is setup correctly please follow the steps below:

- ▶ Get access to the Internet
- ▶ Make sure the 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



- ▶ Select the connection you configured for your Netgear device
- ▶ Hit the **Start VPN** button



- ▶ If the light turns red after a few seconds, then please read the **Troubleshooting** section on the next page
- ▶ If the light turns green, that means you've successfully established a connection

Congratulations! You did it!

Troubleshooting

I don't get a green light in the VPN Tracker main window

- ▶ Make sure that your computer is not connected directly to the office network you want to connect to.
- ▶ Make sure, that the **Identifier** and the **Pre-shared key** you've entered in the router configuration match the settings you entered in VPN Tracker.
- ▶ Verify that the **public IP address** you entered in VPN Tracker matches the public IP address of your router.
- ▶ Download our sample configuration and connect to our test device at <http://www.vpntracker.com/connectiontest/>
 - If the test connection cannot be established: Make sure, that the internet connection is working and verify that your local router is not blocking any connection attempts.
 - If the test connection is established successfully: Your internet connection is working and does not block VPN connections. Please check the VPN log file of your Netgear for error messages.
- ▶ If you're still having issues with your connection, please create some screenshots of your settings on both ends, gather the log files and send them over to our support team via <http://www.equinux.com/us/products/vpntracker/contactus.html>.

What's next?

This section explains how to use your VPN connection.

Introduction

As the VPN connection has now been established, you should be able to access most of the resources in your office network.

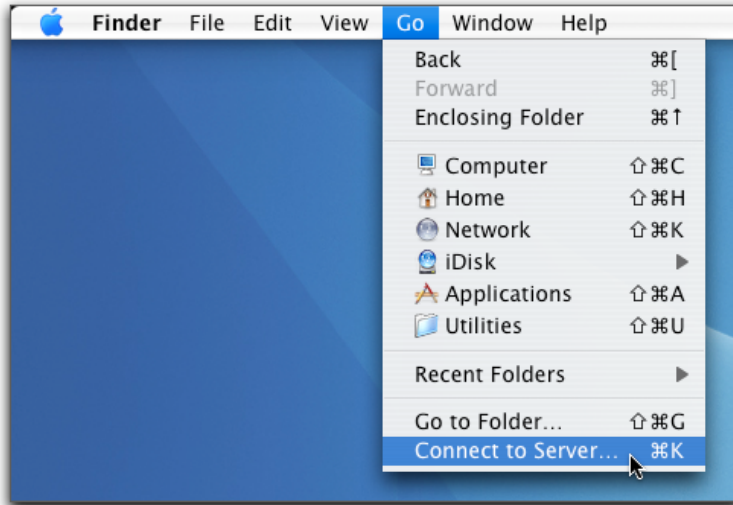
Known Limitations

There are some limitations of a VPN connection compared to a direct connection to a office network.

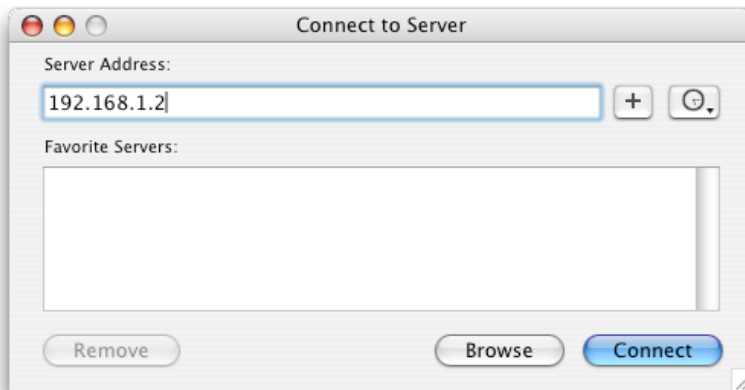
- ▶ **Bonjour:** As Bonjour Chat is not supported over a VPN tunnel, you'll need to use iChat server in order to chat remotely.
- ▶ **Browsing the network:** You can't "browse" the remote network as you're normally used to. You need to connect to each machine manually, as described on the next page.

Accessing Files

To access files in your office network, just follow the steps below:



- ▶ Go to the **Finder** application
- ▶ In the menu bar, click on **Go->Connect To Server...**



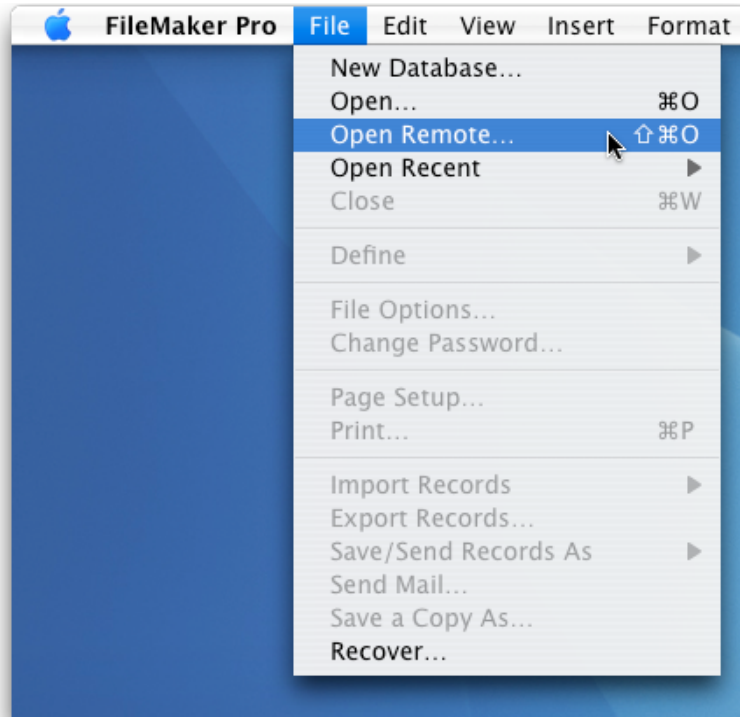
- ▶ Enter the IP address of the machine you want to connect to. In our example network this would be the IP address **192.168.1.2**
- ▶ Click on the **Connect** button
- ▶ Enter your **Username** and **Password** to access the files

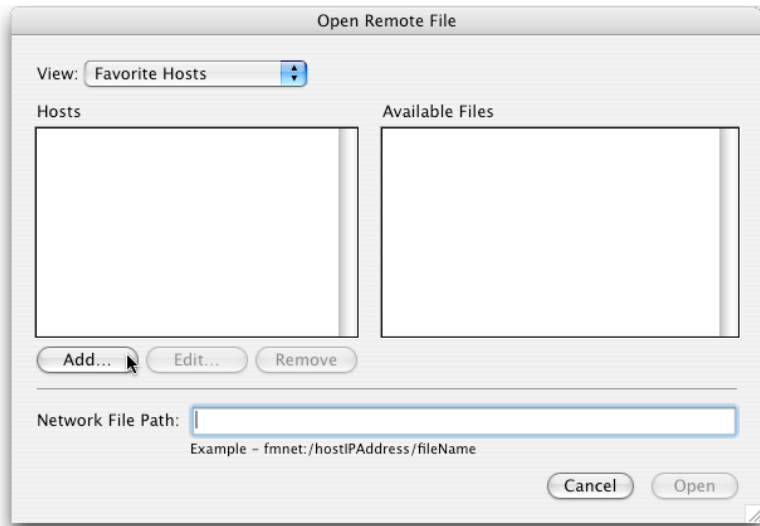
TIP When connecting to a Windows fileserver, you'll need to prefix the IP address with "*smb://*"; e.g. "*smb://192.168.1.2*".

Accessing a FileMaker Database

To access a database available in your office network, just follow the steps below:

- ▶ Start the **FileMaker** application
- ▶ In the menu bar, click on **File->Open Remote...**





► Click on the **Add...** button

Edit Favorite Host

Favorite Settings

Host's Internet Address:
(Example - host.domain.com or 192.168.10.0)

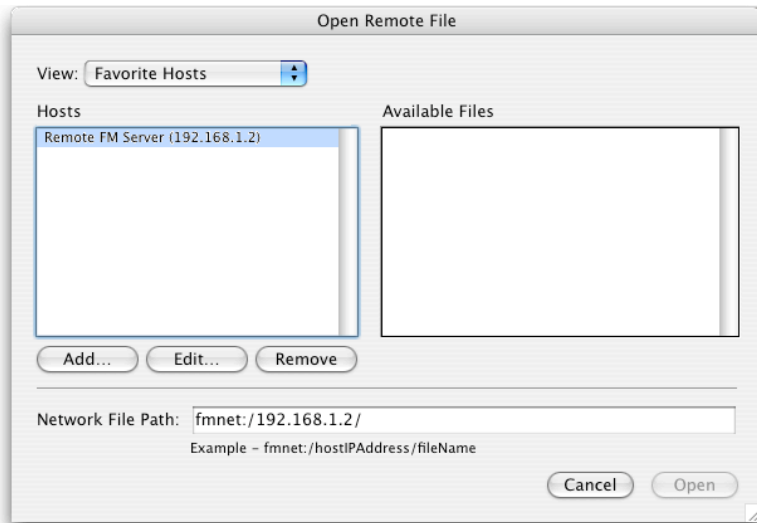
Favorite Host's Name:
(optional)

File Settings

☒ Show all available files for this host
☐ Show only these files

Enter one file name per line, separated by a carriage return

- ▶ Enter the **IP address** of the FileMaker server machine
- ▶ Enter a hostname for this machine (optional)
- ▶ Click on the **Save** button



- ▶ Select a database from the list of **Available Files** and click **Open**
- ▶ You are now able to access your FileMaker databases as usual

Acquire more Licenses

If two or more people need to access your office network via VPN, then you need to acquire more VPN Tracker licenses.

To get more licenses, please contact your reseller and inquire about „VPN Tracker Personal Edition“.

Or point your browser to <http://store.equinux.com> and buy additional VPN Tracker Personal Edition Licenses online.