



VPN Tracker 365

VPN Configuration Guide

NETGEAR® FVS124G

equinux AG and equinux USA, Inc.

© 2015 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.

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.

NETGEAR is a registered trademark of NETGEAR 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.....	4
Important Prerequisites	5
Scenario.....	6
Terminology	7
My NETGEAR Configuration.....	8
Task 1 – Configure your NETGEAR	9
Step 2 – Retrieve your NETGEAR's LAN and WAN Configuration	
11	
Step 3 – Create a new VPN Policy	12
Task 2 – Configure VPN Tracker	14
Step 1 - Create a New Connection	14
Step 2 – Configure the VPN Connection	15
Task 3 – Test the VPN Connection	16
It's time to go out!	16
Start your connection	16
Supporting Multiple Users	18
Using Mode Config for IP Address Assignment	18
Adding more VPN Tunnels	22
Troubleshooting	24
VPN Connection Fails to Establish	24
Cannot Access Resources on the Remote Network	25
Further Questions?	26
VPN Settings Explained	27
IKE Policy	27
VPN Policy.....	30
The Role of the Local Address in VPN Tracker	33

Introduction

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

Note This documentation is only a supplement to, not a replacement for, the instructions included with your NETGEAR device. Please be sure to read those instructions and understand them before starting.

NETGEAR Configuration

The first part of this document will show you how to configure a VPN tunnel on a NETGEAR VPN router using a basic VPN setup that can accept incoming connections from any IP address.

VPN Tracker Configuration

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

Troubleshooting and Advanced Topics

Troubleshooting and advanced topics are covered in the third part of this document. There you will find:

- instructions for setting up a VPN connection for multiple users
- troubleshooting tips
- an in-depth discussion of the various NETGEAR settings and how they relate to VPN Tracker

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, and only add additional features to your connection once you have the basic setup working.

Important Prerequisites

Your NETGEAR Device

This document applies to the following NETGEAR devices

- FVS124G

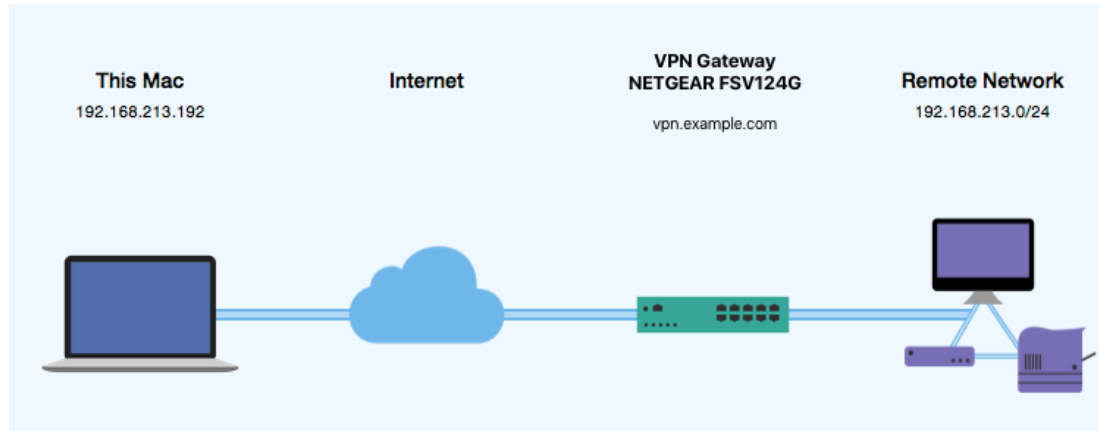
The documentation is based on firmware 1.1.48.

Your Mac

- Make sure to use a recent VPN Tracker version. The latest VPN Tracker release can be obtained from <http://www.vpntracker.com>
- You will need one VPN Tracker license for each Mac running VPN Tracker

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 NETGEAR firewall (the “VPN Gateway”) is also already connected to the Internet and can be accessed through a static IP address or a (Dynamic) DNS host name. In our example setup, we will be using a DNS host name: `vpn.example.com`.

The NETGEAR device 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.

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 NETGEAR Configuration

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 out this form to help keep track of the various configuration settings of your NETGEAR device.

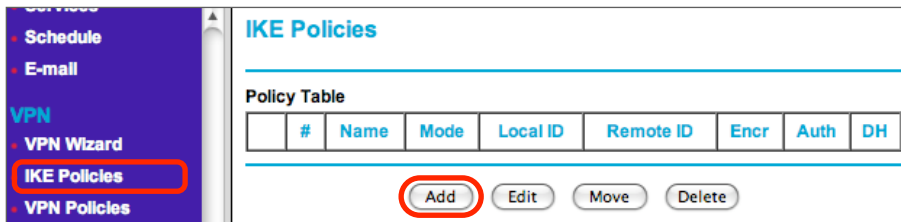
- 1 Pre-Shared Key: _____
- 2 NETGEAR's Local Identifier: _____
- 3 NETGEAR's Remote Identifier: _____
- 4 WAN IP Address: _____ . _____ . _____ . _____ (or DNS host name _____)
- 5 LAN IP Address: _____ . _____ . _____ . _____
- 6 LAN Subnet Mask: _____ . _____ . _____ . _____
- 7 LAN Network Address (calculated, see page 12): _____ . _____ . _____ . _____
- 8 VPN Policy Name: _____

Task 1 – Configure your NETGEAR

This section describes how to set up your NETGEAR's VPN. If you do not yet have VPN configured and in use on your device, please proceed exactly as described in this section. We will first be creating an IKE policy, which corresponds to “Phase 1” in VPN Tracker. In a second step, we will be setting up an associated VPN (IPsec) policy, which corresponds to “Phase 2” in VPN Tracker.

Advanced Users If you already have VPN in use on your device, you can use this chapter to verify your settings (refer to the chapter “VPN Settings Explained” for more detailed information about the settings available on your NETGEAR). If you have multiple VPN policies set up on the device, you will have to ensure that there are no unintended side-effects. Please read the chapter “Supporting Multiple Users” to learn how to set up multiple tunnels without them interfering with each other.

Step 1 – Create a new IKE policy



- ▶ Go to **VPN > IKE Policies**
- ▶ Click “Add”

Note Make sure you have a current backup of your NETGEAR's configuration before making any changes.

IKE Policy Configuration

General

Policy Name:

Direction/Type:

Exchange Mode:

Local

Select Local Gateway: ☐ WAN 1 ☐ WAN 2

Local Identity Type:

Local Identity Data: ❷

Remote

Remote Host Configuration Record: ☐ None ☒ None

Remote Identity Type:

Remote Identity Data: ❸

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method: ☒ Pre-shared Key

❶

☐ RSA Signature (requires Certificate)

Diffie-Hellman (DH) Group:

SA Life Time: (secs)

- **Policy Name:** Enter a name for the connection
- **Direction / Type:** Select “Responder”
- **Exchange Mode:** Select “Aggressive Mode”
- **Local Identity Type:** Select “Fully Qualified Domain Name”
- **Local Identity Data:** Enter the identifier to be used by the device, e.g. “netgear.local”. Make sure to write down the **exact** identifier ❷
- **Remote Identity Type:** Select “Fully Qualified Domain Name”
- **Remote Identity Data:** Enter the identifier to be used by the client, e.g. “vpntracker.local”. It should **not** be an actually existing name. Make sure to write down the **exact** identifier ❸

Advanced Users You *can* use an existing FQDN if your clients actually connect from the IP address this name resolves to.

- **Encryption Algorithm:** Select “3DES”
- **Authentication Algorithm:** Select “SHA-1”
- **Authentication Method:** Select “Pre-Shared Key”
 - The pre-shared key is the password that users have to enter before connecting. Make sure to set a strong password ❶
- **Diffie-Hellman (DH) Group:** Select “Group 2 (1024 Bit)”
- **SA Lifetime:** 3600 seconds
- Click “Apply” to add your new IKE policy

Tip Use the form on page 9 of this document to keep track of the various settings. You will need again them later on.

Step 2 – Retrieve your NETGEAR's LAN and WAN Configuration

Router Status	
System Name	FVS124G
Firmware Version	V1.1.48
LAN Port	
MAC Address	00:0F:B5:00:00:00
IP Address	192.168.13.1 ⁵
DHCP	disabled
IP Subnet Mask	255.255.255.0 ⁶
WAN1 Configuration	
WAN Mode	rollover-primary
WAN State	Up
NAT (Network Address Translation)	enabled
Connection Type	STATIC
Connection State	Up
IP Address	194.145.236.2 ⁴
Subnet Mask	255.255.255.192
Gateway	194.145.236.1
Primary DNS	194.145.236.1
Secondary DNS	0.0.0.0
MAC Address	00:0F:B5:00:00:00

(*) If you are using a subnet mask with elements that are not 0 or 255, you can use one of the many subnet calculators available for free on the Internet to calculate the network address.

► Go to **Maintenance > Router Status** and obtain the following information from the Router Status page:

► **WAN1 Configuration:**

- Write down the **WAN IP Address** ⁴
- If you use Dynamic DNS for your device, or if it has a DNS host name, write down the host name instead

► **LAN Port:**

- Write down the **LAN IP Address** ⁵
- Write down the **LAN IP Subnet Mask** ⁶

► Calculate your **LAN Network Address** by applying the **LAN Subnet Mask** ⁶ to the **LAN IP Address** ⁵:

► 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 ⁷

Step 3 – Create a new VPN Policy

VPN Policies

Policy Table

#	Enable	Name	Type	Local	Remote	AH	ESP
---	--------	------	------	-------	--------	----	-----

VPN Client Policies

Policy Table

#	Enable	Name	Type	Local	Remote	AH	ESP
---	--------	------	------	-------	--------	----	-----

VPN - Auto Policy

General

Policy Name:

IKE policy:

Remote VPN Endpoint: Address Type: Address Data:

SA Life Time: (Seconds) (Kbytes)

☐ IPsec PFS PFS Key Group:

► Go to **VPN > VPN Policies**

► Click “Add Auto Policy”

► **VPN Policy Name:** Enter a name for the VPN Policy ⑧. You can use the same name you used for the IKE policy.

► **IKE Policy:** Select the IKE Policy you have just created

► **Remote VPN Endpoint:** Select “Fully Qualified Domain Name”, and enter the same identifier here that you used as the Remote Identity ③ in the IKE policy

► **SA Life Time:** 3600 seconds / 0 Kbytes

► **IPsec PFS:** Keep IPsec PFS turned off

► **PFS Key Group:** Keep the selected “Group 1 (768 Bit)”

Advanced Users You can turn on Perfect Forward Secrecy (PFS) later, if you wish. The setting on the device must match the setting in VPN Tracker (Advanced > Phase 2 > Perfect Forward Secrecy).

Traffic Selector

Local IP

Subnet address: Subnet address

Start IP address: 192 . 168 . 13 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Remote IP

Any

Start IP address: 0 . 0 . 0 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

AH Configuration

☐ Enable Authentication

Authentication Algorithm: SHA-1

ESP Configuration

☒ Enable Encryption

Encryption Algorithm: 3DES

☒ Enable Authentication

Authentication Algorithm: SHA-1

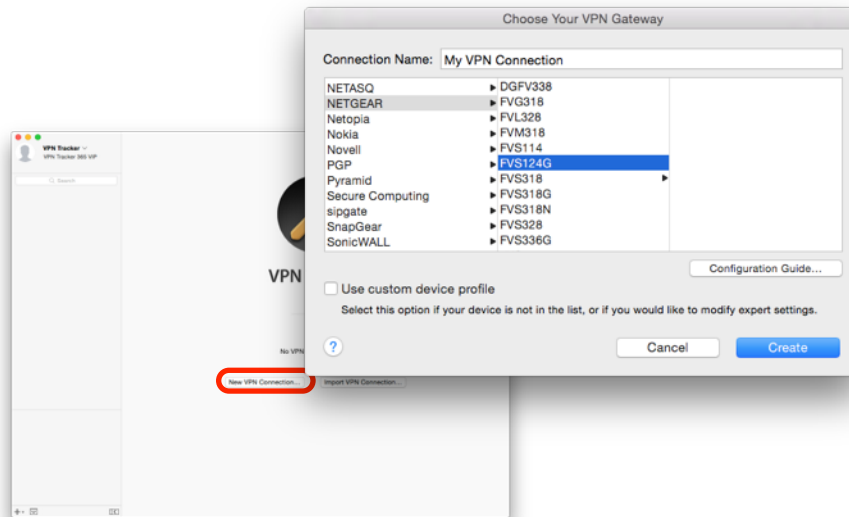
Back Apply Cancel

- **Local IP:** Select “Subnet Address”
- **Start IP address:** Enter the LAN Network Address **7** you calculated in Step 2 (here: 192.168.13.0)
- **Subnet Mask:** Enter the LAN subnet mask **6** you wrote down in Step 2 (here: 255.255.255.0)
- **Remote IP:** Select “Any”
- **AH Configuration:** Leave this setting turned off
- **ESP Configuration**
 - **Enable Encryption:** Turn on encryption
 - **Encryption Algorithm:** Select “3DES”
 - **Enable Authentication:** Turn on authentication
 - **Authentication Algorithm:** Select “SHA-1”
- Click “Apply” to add your new VPN policy

Task 2 – Configure VPN Tracker

This section describes how to configure VPN Tracker to connect to your NETGEAR. You will need the configuration information you collected during Task 1. If you are missing any information, please refer back to “Task 1 – Configure your NETGEAR”.

Step 1 - Create a New Connection



- ▶ Start VPN Tracker
- ▶ Click the “+” button at the bottom of the connection list

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

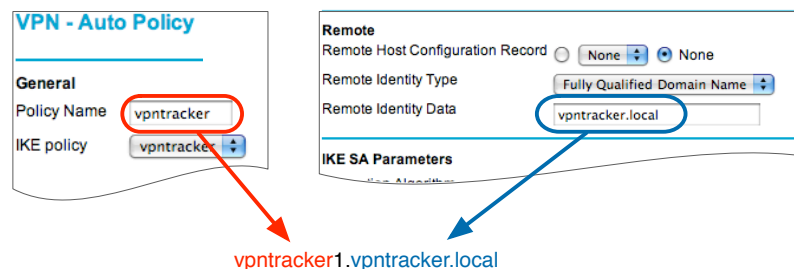
- ▶ Select “**Netgear**” from the list
- ▶ Select your device from the list of NETGEAR devices
- ▶ If your device has more than one device or firmware revision available, be sure to select the revision/firmware matching your device
- ▶ **Connection Name:** Choose a name for your connection (e.g. “Office”)
- ▶ Click “OK”

Step 2 – Configure the VPN Connection

The screenshot shows the Netgear VPN configuration interface. Key fields and their values are as follows:

- Connection Name:** My VPN Connection
- Connection based on:** NETGEAR FVS124G Configuration Guide
- VPN Gateway:** vpn.example.com (callout 4)
- Network Configuration:**
 - Topology: Host to Network
 - Local Address: IP Address
 - Remote Networks: 192.168.13.0 / 24 (callouts 6 and 7)
- Authentication:** Pre-shared key (Pre-shared key not saved)
- Identifiers:**
 - Local: Fully Qualified Domain Name (FQDN) Vpntracer1.vpntracer.local (callouts 8 and 2)
 - Remote: Fully Qualified Domain Name (FQDN) netgear.local (callout 3)
- DNS:** ☐ Use Remote DNS Server

(*) How to build the **Local Identifier**:



- ▶ **VPN Gateway:** Enter your NETGEAR's public IP address **4**. 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:** Leave empty for now. Depending on your setup, you may have to set a specific Local Address eventually. Refer to "Supporting Multiple Users" for details
- ▶ **Remote Networks:** Enter the network address **7** and the subnet mask **6** of the network that is being accessed through the VPN tunnel. Separate the subnet mask with a forward slash ("/")
- ▶ **Identifiers**
 - ▶ Make sure the types for both identifiers are set to "**Fully Qualified Domain Name (FQDN)**"
 - ▶ **Local:** The local identifier consists of the NETGEAR's VPN policy name **8**, a number between 1 and 10 (different for each user of this connection), and the NETGEAR's remote identifier **3** (see the diagram on the left). In our example, the local identifier is "vpntracer1.vpntracer.local"
 - ▶ **Remote:** Enter the **local** identifier from your NETGEAR (e.g. "netgear.local") **2**

Task 3 – Test the VPN Connection

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

It's time to go out!

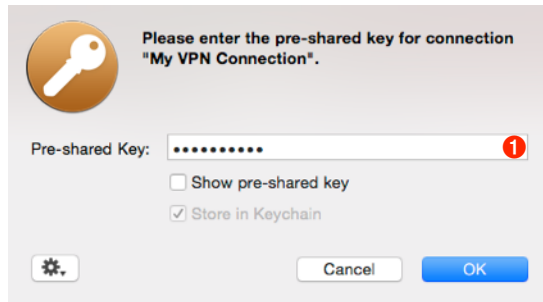
You will not be able to test and use your VPN connection from within the internal network that you want to connect to. To test your connection, you will need to connect from a different location. For example, if you are setting up a VPN connection to your office, test it from home. If you are setting 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 NETGEAR device ❶
- ▶ 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 blue after a while, you have successfully established a connection



Congratulations!

Supporting Multiple Users

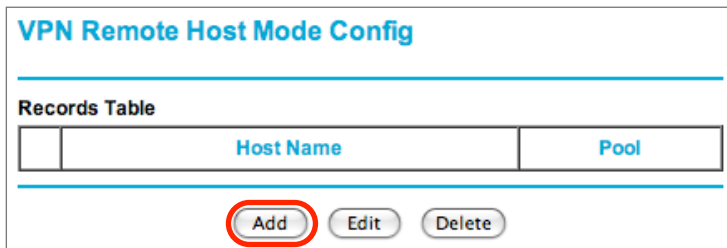
Once your VPN expands to multiple users, you must ensure that IP addresses do not conflict. In addition to such purely technical considerations, VPN Tracker makes it easy to distribute pre-configured connections to your users, and prevent the modification of VPN connections and access to confidential data.

Using Mode Config for IP Address Assignment

If multiple users connect using the same policy on your NETGEAR 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. The easiest way to ensure this, is to automatically have the NETGEAR assign IP addresses to connecting clients through Mode Config.

Note If you cannot use Mode Config for distributing IP addresses, please refer to “The Role of the Local Address in VPN Tracker” for alternative solutions.

Creating an Address Pool for Mode Config



VPN Remote Host Mode Config

Records Table

	Host Name	Pool
--	-----------	------

Add Edit Delete

- Go to “VPN > ModeConfig”
- Click “Add”

VPN Remote Host Configuration Record

General

Record Name

First IP Pool

Second IP Pool

Third IP Pool

First WINS server

Second WINS server

First DNS server

Second DNS server

Traffic Tunnel Security Level:

PFS

Local Address 7

Local Subnet Mask 4

SA Lifetime

Traffic Tunnel Security Level:

Authentication Algorithm

Encryption Algorithm

- **Record Name:** Enter a name that will later allow you to recognize this entry
- **First IP Pool:** Enter an IP range that is **not** part of your NETGEAR's LAN. The range must be from the private ([RFC1918](#)) IP address space, and it should be large enough to accommodate at least the maximum number of simultaneous VPN connections expected
- **Second/Third IP Pool** (optional): It is possible to add more pools, if required
- **First/Second WINS server** (optional): The WINS servers are not used by VPN Tracker and therefore can remain empty
- **First/Second DNS Server** (optional): If you operate your own DNS server, enter it here. Otherwise, these fields should remain empty
- **Traffic Tunnel Security Level:** These settings correspond to the VPN Policy settings of the same name. The screenshot shows the default settings used by a normal (non Mode Config) VPN policy. Since these match the settings pre-configured in VPN Tracker, it is a good idea to use them for now. You will need to customize the following settings according to your specific configuration (refer to “ Step 2 – Retrieve your NETGEAR's LAN and WAN Configuration” for the specific values that you will have to enter):
 - **Local Address:** Enter the LAN Network Address 7 calculated earlier,
 - **Local Subnet Mask:** Enter the LAN subnet mask 4 of your NETGEAR
- Click “Apply” to add the new address pool

Delete the VPN Policy

VPN Client Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	AH	ESP
	1	<input checked="" type="checkbox"/>	vpntracker	Auto	192.168.13.0/255.255.255.0	ANY	Disabled	Enabled

- ▶ The VPN policy must be removed before you can change the IKE policy to use Mode Config
- ▶ Go to “**VPN > VPN Policies**”
- ▶ Select your VPN Policy
- ▶ Click “Delete”

Configure the IKE Policy to use Mode Config

IKE Policies

Policy Table

	#	Name	Mode	Local ID	Remote ID	Encr	Auth	DH
	1	vpntracker	Aggressive	netgear.local	vpntracker.local	3DES	SHA1	Group 2 (1024 Bit)

- ▶ Go to “**VPN > IKE Policies**”
- ▶ Select your IKE Policy
- ▶ Click “Edit”

Remote

Remote Host Configuration Record

Remote Identity Type

Remote Identity Data

☒ vpntracker ☐ None

Fully Qualified Domain Name

vpntracker.local

- ▶ In the “**Remote**” section, select “**Remote Host Configuration Record**”
- ▶ Select the record you created earlier
- ▶ Click “Apply”

Enable Mode Config in VPN Tracker

Connection based on Need help?	NETGEAR FVS124G Configuration Guide
VPN Gateway	vpn.example.com ?
Network Configuration	Mode Config ?
Topology	Host to Network ?
Remote Networks	Network Address ?

- ▶ Check “**Mode Config**” in the “**Network Configuration**” section. If you cannot find this setting for your device, make sure you have selected the correct device and firmware revision

Advanced Users It is very important to initially set up Mode Config as “automatic” instead of “active” or “passive”. While this may mean a short delay when connecting (if the device actually requires “active” mode config), it will ensure that it works in both cases. You can later try passive or active to see which mode your device and particular firmware revision actually uses

Adding more VPN Tunnels

The tunnel you have set up in the first part of this document can be used by multiple users if you use Mode Config (with a sufficiently large IP address pool), or if you manually set an individual Local Address for each user, as described in “The Role of the Local Address in VPN Tracker”. **This is the recommended setup.**

However, there may be situations where it is necessary to create additional VPN tunnels, instead of reusing one tunnel. For example, if you need to issue users individual pre-shared keys, you can add multiple VPN tunnels with different pre-shared keys. Or you may require a static gateway-to-gateway tunnel, in addition to a tunnel used by VPN clients.

Tip If your needs expand to more than a handful of users, you may want to consider upgrading to a VPN gateway that supports Extended Authentication (XAUTH) in order to avoid having to set up an individual VPN tunnel on the device for each user, just to be able to issue them individual passwords.

When more than one tunnel is configured and enabled on the device, you will have to ensure that there are no conflicts:

- For the IKE policies, make sure that the identifiers for each tunnel are different.
- If you have more than one tunnel used by clients connecting from dynamic IP addresses, make sure that the “Remote IP” is “Any” for **only one** of the policies (or simply use Mode Config). If you are using an “Any” policy, it must be last in the list. For the other tunnels, set a fixed remote IP that is the same as the “Local Address” in VPN Tracker. In the following example, the address “10.22.13.1” is used both on the device and in VPN Tracker:

Remote IP	Single address
Start IP address:	10 . 22 . 13 . 1
Finish IP address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0

Network	Host to Network
VPN Gateway	vpn.example.com
Local Address	10.22.13.1
Remote Networks	192.168.13.0 / 255.255.255.0

Note A VPN policy that is set up to accept only a single “Remote IP” can only be used by a single user at a time.

If you have difficulties setting up multiple tunnels on a single device, it is a good idea to check the VPN Status (VPN > VPN Status > VPN Status) to see which policies are in use. If necessary, selectively disable policies to see which policies are causing trouble.

Note Please refer to your device's data sheet to find out the maximum number of VPN tunnels that can be set up on your device.

Troubleshooting

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

VPN Connection Fails to Establish

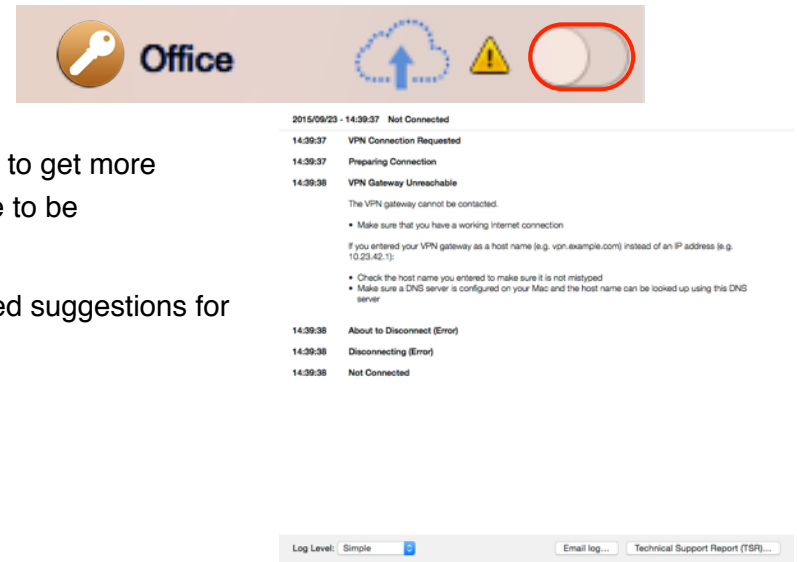
On/Off Slider goes back to “Off” right away

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 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. You can also 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.



Cannot Access Resources on the Remote Network

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

Connect by IP address instead of host name

If you are not connecting to the resource by IP address (e.g. 192.168.13.42), 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 the DNS server configured on your Mac's is able to resolve this host name to an IP address, or configure a "Remote DNS" server in VPN Tracker.

Run the VPN Environment Manager

In many local 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 one of three different methods, but not all of them may be supported by your local router or your VPN gateway. In that case, your VPN connection may seem connected, but no connections to servers or other resources in the VPN are possible. VPN Tracker includes a tool to detect the right method for the local network:

- Stop all running VPN connections
- Select "Help > VPN Environment Manager"
- Click on "Continue"
- Wait until VPN Tracker has performed the tests
- Try to start the connection again

Tip You will only have to run the VPN Environment Manager once for each location that you are using VPN Tracker at.

Check whether the IP address is part of the remote network

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

Tip The network mask (e.g. 255.255.255.0) determines the size of a network. Some examples: The network 192.168.1.0/255.255.255.0 contains **all** IP addresses starting with 192.168.1.x. The network 192.168.1.0/255.255.255.**255** contains only a single IP address, 192.168.1.0.

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

VPN Settings Explained

This section explains the various settings found on your NETGEAR, and how they relate to VPN Tracker's settings. We will first go through the IKE policy settings from top to bottom, then through the VPN policy settings. In the end, a few selected VPN Tracker settings that have no matching setting on the NETGEAR, or are found elsewhere, are explained.

IKE Policy

The IKE Policy contains the settings for the first phase in the process of establishing a VPN connection. **Many of the settings here correspond to settings located in VPN Tracker on the Basic tab, or under Advanced > Phase 1.**

General

General	
Policy Name	<input type="text" value="vpntracker"/>
Direction/Type	<input type="button" value="Responder"/>
Exchange Mode	<input type="button" value="Aggressive Mode"/>

Policy Name: The policy name is used only for naming connections on the device. Use a name that you will recognize later.

Direction / Type: Must be “**Responder**” for VPN clients to be able to connect.

Exchange Mode: Always use “**Aggressive**” Mode if VPN clients connect from dynamic IP addresses. The Exchange Mode configured here must match the Advanced > Exchange Mode setting in VPN Tracker. If you must for some reason use Main Mode here, please refer to your device's documentation for any prerequisites for using Main Mode.

Local and Remote Identifier

Local	
Select Local Gateway	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2
Local Identity Type	Fully Qualified Domain Name
Local Identity Data	netgear.local
Remote	
Remote Host Configuration Record	<input type="radio"/> None <input checked="" type="radio"/> None
Remote Identity Type	Fully Qualified Domain Name
Remote Identity Data	vpntracker.local

Select Local Gateway: If the device has more than one active WAN interface, select the interface to be used for VPN. You must configure this WAN interface's IP address in VPN Tracker as the VPN Gateway.

Local Identity Type: The local identity's type on the device must match the **Remote** Identifier Type (Basic > Identifiers) in VPN Tracker.

Local Identity Data: The local identity data on the device must match the **Remote** Identifier (Basic > Identifiers) in VPN Tracker.

Remote Host Configuration Record: When Mode Config is used, select the appropriate Mode Config record here.

Remote Identity Type: The type set on the device must match the **Local** Identifier Type (Basic > Identifiers) in VPN Tracker.

Remote Identity Data: The remote identity data on the device must match the **Local** Identifier (Basic > Identifiers) in VPN Tracker.

Note For a VPN policy where the Traffic Selector is set to “**Any**” for the Remote IP, a **special Local Identifier** must be used in VPN Tracker. It is constructed from the VPN policy name, a number between 1 and 10, and the Remote Identity Data configured on the NETGEAR (refer to page 16 for an example).

IKE SA Parameters

Encryption Algorithm: The encryption algorithm must match the encryption algorithm configured in VPN Tracker in Advanced > Phase 1 > Encryption Algorithms. The device uses 3DES by default, which is generally a good choice. AES-128/192/256 are considered to be even more secure (AES-192/AES-256 are only available in the Professional Edition of VPN Tracker).

IKE SA Parameters	
Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Authentication Method	<input checked="" type="radio"/> Pre-shared Key <input type="radio"/> RSA Signature (requires Certificate)
	topsecret
Diffie-Hellman (DH) Group	Group 2 (1024 Bit)
SA Life Time	3600 (secs)

Note While is possible to set more than one encryption algorithm in VPN Tracker (as long as the one actually used by the device is among them), setting more than two or three algorithms (or algorithms not known to the device) may cause the connection to fail.

Authentication Algorithm: The authentication algorithm must match the hash algorithm configured in VPN Tracker (Advanced > Phase 1 > Hash Algorithms). Do not select more hash algorithms in VPN Tracker than the one selected on the device.

Authentication Method: Unless you already have a Public-Key Infrastructure (PKI) in place for your users, you will probably want to start out using pre-shared key (i.e. password-based) authentication. The method must match Basic > Authentication in VPN Tracker.

Pre-shared key: This is the password for the VPN connection, and corresponds to the same setting in VPN Tracker (Basic > Authentication). This password is shared among all users. Make sure to choose a strong password here that is long enough and contains a mix of letters and numbers (but be aware that your Mac and your NETGEAR may not use the same character encoding, so try to avoid accented characters).

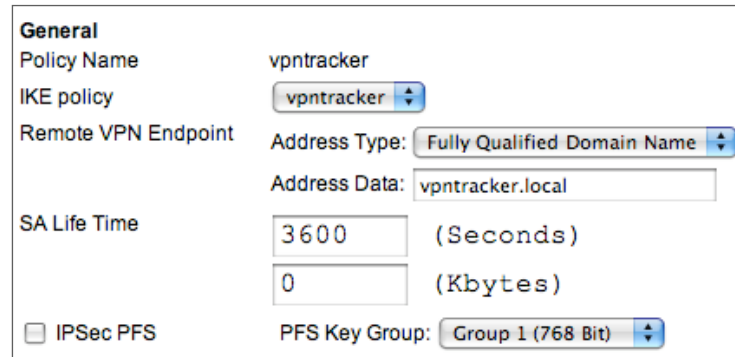
Diffie-Hellman (DH) Group: The Diffie-Hellman (DH) group defined here must match the group selected for phase 1 in VPN Tracker (Advanced > Phase 1 > Diffie-Hellman). Using a longer key (= higher number) is more secure, but may also be slower.

SA Life Time: The IKE SA lifetime indicates when the phase 1 of the connection needs to be re-established. The lifetime must match the lifetime for phase 1 in VPN Tracker (Advanced > Phase 1 > Lifetime). A value of 3600 sec (1 hour) or more is generally a good choice.

VPN Policy

The VPN Policy contains the settings for the second phase in the process of establishing a VPN connection. **Many of the settings here correspond to settings located in VPN Tracker in the Network section of the Basic tab, or in Advanced > Phase 2.**

General



The screenshot shows the 'General' tab of a VPN Policy configuration window. The settings are as follows:

Field	Value
Policy Name	vpntracker
IKE policy	vpntracker
Remote VPN Endpoint	Address Type: Fully Qualified Domain Name Address Data: vpntracker.local
SA Life Time	3600 (Seconds) 0 (Kbytes)
<input type="checkbox"/> IPSec PFS	PFS Key Group: Group 1 (768 Bit)

Policy Name: The policy name is used for naming connections on the device. For a policy where “Traffic Selector > Remote IP” is set to “Any”, the policy name also becomes part of VPN Tracker’s Local Identifier.

IKE Policy: Select the corresponding IKE policy. An IKE policy that is not selected in any VPN policy cannot be accessed. However, selecting an IKE policy here does not automatically mean that connections from the selected IKE policy will use this VPN policy, the VPN policy lookup on this device is independent

from the IKE policy and determined by the traffic selectors.

Remote VPN Endpoint: This is the (public) IP address of the connecting client. With clients connecting from different IP addresses, it should be set to “Fully Qualified Domain Name”. Enter the same Fully Qualified Domain Name (FQDN) that is used for the “Remote Identity Data” in the IKE Policy.

SA Life Time: The lifetime determines how long a client can be connected before the encryption keys must be renegotiated. The lifetime must match the lifetime for phase 2 in VPN Tracker (Advanced > Phase 2 > Lifetime). A value of 3600 sec (1 hours) or more is generally a good choice. Due to the complications involved with a lifetime that depends on data transfer amounts, we recommend setting the lifetime in “Seconds” only, and setting the “Kbytes” field to 0.

IPsec PFS: The setting must match the Perfect Forward Secrecy (PFS) setting in VPN Tracker (Advanced > Phase 2 > Perfect Forward Secrecy (PFS)). Turning on PFS provides additional security.

IPsec PFS Key Group: The PFS key group must match the PFS Diffie-Hellman (DH) group in VPN Tracker (Advanced > Phase 2 > Perfect Forward Secrecy (PFS)).

Traffic Selector

Local IP	Subnet address
Start IP address:	192 . 168 . 13 . 0
Finish IP address:	0 . 0 . 0 . 0
Subnet Mask:	255 . 255 . 255 . 0
Remote IP	Any
Start IP address:	0 . 0 . 0 . 0
Finish IP address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0

The Traffic Selection settings determine the endpoints of the VPN tunnel.

►The **local** (=NETGEAR) side of the tunnel should be configured to be a subnet matching the NETGEAR's LAN (192.168.13.0/255.255.255.0 is the NETGEAR's LAN in our example)

►The **remote** part should be set to "Any".

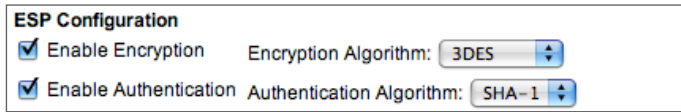
Advanced Users If you are not setting the remote part of the Traffic Selection to "Any" (for example, because you have different VPN policies all used by clients connecting from dynamic IP addresses), it must match exactly what is configured in VPN Tracker as the Local Address (or Local Network, if using a Network to Network connection). Range type addresses are not supported in VPN Tracker.

AH Configuration

AH Configuration	
<input type="checkbox"/> Enable Authentication	Authentication Algorithm: SHA-1

Enable Authentication: VPN Tracker uses Encapsulating Security Payload (ESP) with authentication. Using Authentication Header (AH) is not necessary and not supported. It should be turned off.

ESP Configuration



ESP Configuration

☒ Enable Encryption Encryption Algorithm: 3DES

☒ Enable Authentication Authentication Algorithm: SHA-1

Enable Encryption: This setting ensures that data transferred through the VPN tunnel is encrypted. It should always be turned on, and must match the corresponding setting in VPN Tracker (Advanced > Phase 2 > Encryption Algorithms).

The device uses 3DES by default, which is generally a good choice. AES-128/192/256 are considered to be even more secure (AES-192/AES-256 are only available in the Professional Edition of VPN Tracker).

Note While it is possible to set more than one encryption algorithm in VPN Tracker (as long as the one used by the device is among them), setting more than two or three algorithms (or algorithms not known to the device) may cause the connection to fail

Enable Authentication: This setting ensures that data sent through the VPN tunnel is authenticated. It should always be turned on, and must match the corresponding setting in VPN Tracker (Advanced > Phase 2 > Authentication Algorithms). Do not select more authentication algorithms in VPN Tracker than the one selected on the device. NETGEAR uses SHA-1 by default (which corresponds to HMAC SHA-1 in VPN Tracker, MD5 on the NETGEAR corresponds to HMAC MD5 in VPN Tracker).

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
- ▶ When Mode Config is used, the Local Address is assigned automatically by the VPN gateway

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

If Mode Config is not being used, it is beneficial to use fixed Local Addresses in VPN Tracker, instead of leaving the Local Address field empty. **Always use a fixed Local Address if:**

- ▶ multiple clients (users/computers) use the VPN, and you cannot use Mode Config (see "Supporting Multiple Users")
- ▶ the NETGEAR device is not the default gateway (router) in the remote network

Choosing the Local Address

When connecting to a NETGEAR device, the Local Address **must not be part of the remote network** (i.e. the NETGEAR'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 NETGEAR's LAN in this example is the network 192.168.13.0/24 (= 192.168.13.0/255.255.0). 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 NETGEAR's LAN?

It may sound a bit unusual to use IP addresses that are not part of the NETGEAR's LAN. The reason for this is that the NETGEAR cannot act as a so-called "ARP Proxy" for its VPN clients. Computers on the NETGEAR's LAN therefore must be "tricked" into sending replies for VPN clients to the NETGEAR 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 such 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 choices), 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 have to set a fixed Local Address when my NETGEAR is not the default gateway (router) in its LAN?

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

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 NETGEAR 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 NETGEAR