VPN Tracker Manual

Version 5

equinux AG and equinux USA, Inc.

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

equinux shall have absolutely no liability for any direct or indirect, special or other consequential damages in connection with the use of the manual 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.

Disclaimer

You agree that equinux USA, Inc. shall have no liability whatsoever for any use you make of the Software. You shall indemnify and hold harmless equinux USA, Inc. from any third party claims, damages, liabilities, costs and fees (including reasonable attorney fees) arising from your use of the Software as well as from your failure to comply with any term of this Agreement.

Welcome to VPN Tracker!

Thank you for your selection of the leading VPN client for the Mac. If you are new to VPN, we recommend you read this chapter to familiarize yourself with the basic concepts of Virtual Private Networks.

What is a VPN?

VPN is an abbreviation of **Virtual Private Network**. A VPN connection is established between two peers (e.g. a Mac running VPN Tracker and a VPN gateway). These peers negotiate a so-called "Security Association" which is used to encrypt and authenticate the data transferred between them. This ensures that the data

- cannot be read by a 3rd party (**confidentiality**)
- cannot be changed by a 3rd party (**integrity**)
- is known to originate from the remote peer (**authenticity**)

What is a VPN Gateway?

The general term "gateway" describes a device which handles external network traffic for a computer (or several computers in a local network). Such devices are also called routers, and many of them include security features (which turns them into a "firewall"). A gateway has at least two interfaces – a local or private interface is used by the computers on its local area network (LAN), and a public interface which is connected to the Internet. Both interface can be wired (using Ethernet cables) or wireless (using Airport/WLAN or 3G wireless connections).

If a gateway is capable of handling a VPN connection, it is called a VPN gateway. VPN gateways are usually specialized hardware devices from vendors like Cisco, SonicWALL, or Netgear. In some cases, VPN functionality is provided by some software running on a standard computer (e.g. Astaro Internet Security), which turns this computer into a VPN gateway.

In this guide, we will talk about VPN gateways, or simply VPN devices.

What is VPN Tracker?

VPN Tracker is a versatile, user-friendly VPN client for Mac OS X. Using a collection of industry-standard algorithms (the IPSec standard, and some extensions), VPN Tracker can secure all your internet-based communications, including those over wireless networks.

VPN Tracker should work with all VPN gateways implementing the above standard (IPSec) properly. Our predefined device profiles for a large variety of VPN gateways make setting up secure, encrypted tunnels to remote networks easier than ever before!

Note Please refer to the chapter "Device Profiles" if you cannot find a device profile for the gateway you'd like to use.

What can I use a VPN connection for?

A VPN allows you to access a remote network (e.g. your office network, or your Mac at home) securely from anywhere in the world, through the Internet. You can download and upload files, receive mails from your company's mail server, manage computers remotely, or access FileMaker databases.

Where can I use my VPN connection?

All you need to establish and use a VPN connection is a working Internet connection at both ends. Whether you're working from a hotel, an Internet cafe or from your home office, VPN Tracker will contact your VPN gateway at its public interface, and negotiate the VPN connection.

Note In some cases, local routers may interfere. Please use the VPN Environment Manager (from the "Help" menu) to check your network environment.

Need More Info?

More info on Virtual Private Networks and the IPSec technology can be found in the chapter "IPSec Explained".

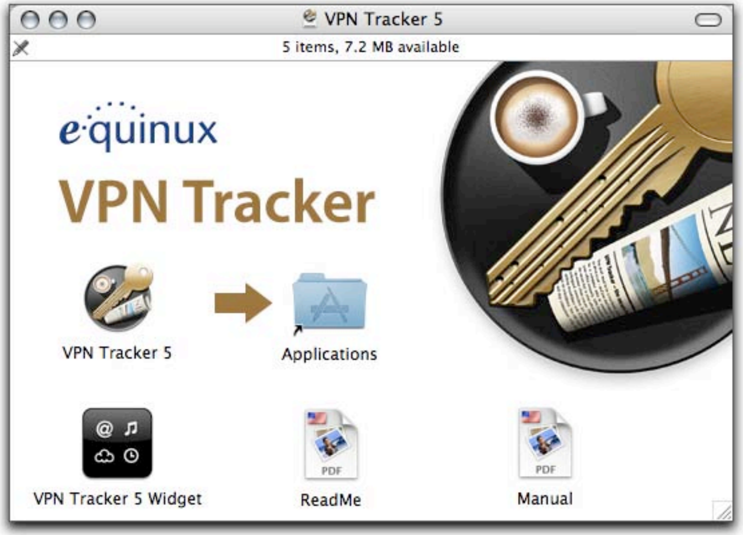
Installation

Install VPN Tracker

The first step is to install VPN Tracker on your Mac.

To install VPN Tracker on your Mac:

- Download VPN Tracker from the equinux web site at http://www.equinux.com/vpntracker/download
- If the downloaded disk image is not mounted automatically, double-click the file



- Drag the VPN Tracker application symbol into your ”Applications” folder
- Eject the disk image by dragging it to the trash

You can now use VPN Tracker in demo mode – all connections will be terminated after three minutes. If you already tested the software, you should activate the application right away.

Activate VPN Tracker

Activating VPN Tracker is a simple and straightforward process. Described below are three different scenarios: Buy a new license online, activate a retail version and transfer a license.

Note Your equinux ID will be used to store and manage all your licenses. Whenever you purchase additional licenses or other products, please specify your equinux ID.

Buy a License

Obtaining a license for VPN Tracker and activating it on your Mac is a simple process.

To buy a license, please complete the following steps:

- Choose “VPN Tracker“ > “Buy VPN Tracker...“
- Click “Buy VPN Tracker”
- If you are a new customer, choose your country and click “Next“.

or

- If you already registered with equinux, login with your equinux ID
- Choose the desired license
- Click "Check Out"
- Continue shopping for other equinux products

or

- Click "Continue Check Out"
- If you are a new customer, register a new equinux ID
- Select either "Bank Transfer", "PayPal" or "Credit Card" as your preferred payment option
- Enter your credit card data, if necessary
- Review your order and click "Complete Order"

If you paid with PayPal, you will be redirected to the PayPal website to make your payment.

If your PayPal or credit card payment is authorized immediately, VPN Tracker will be activated automatically. Your license will be stored on your Mac.

If you paid by bank transfer, you will be sent an email with payment instructions. As soon as we receive your payment, we will add the license to your equinux ID and notify you by email. You can then use your equinux ID and password to activate the software.

To activate VPN Tracker with your equinux ID:

- Select "VPN Tracker > Activate VPN Tracker..."
- Click "Activate VPN Tracker"
- Enter your equinux ID and password
- Click "Login" and follow the instructions

Activate a Retail Version

If you bought a retail version of VPN Tracker at your local software store, you received an "Activation Code". This code can be used to create a license.

To activate a retail version, please complete the following steps:

- Choose "VPN Tracker 5" > "Activate VPN Tracker..."
- Click "Activate VPN Tracker"
- Register a new equinux ID (if this is your first equinux product)

or

- Login with your equinux ID
- Enter your Activation Code

Your license will be created and stored on your Mac automatically.

Transfer a License

All licenses for equinux products are hardware bound. When registering our software on your computer, the license is created for this machine. This means that a license can only be used on a single computer.

However, transferring a license to a different computer is easy.

To transfer a license, please complete the following steps:

- On your old Mac, choose "VPN Tracker 5" > "Deactivate VPN Tracker"

The license will now be available for activating the software on your new Mac.

- Install VPN Tracker on your new Mac

- On your new Mac, activate VPN Tracker with your equinux ID (s. above)

VPN Tracker will automatically fetch the free license.

> **Note** From now on, the software cannot be used on the old machine. To transfer the license back, just reverse the process described above.

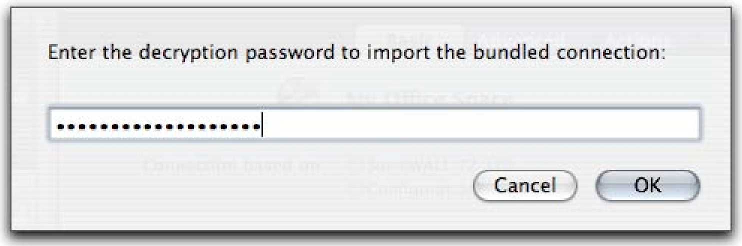
Installing a Deployment Bundle

If your administrator provided a deployment bundle, installation, activation, and configuration can be completed in a single step.

> **Note** Installing a deployment bundle requires Internet access and an administrator password on your Mac.

- Double-click the deployment bundle (a disk image) to open it
- Copy the VPN Tracker application to your Applications folder
- Eject the disk image by dragging it to the Trash
- Double-click the application icon

VPN Tracker will ask you to enter the decryption password sent to you by your administrator

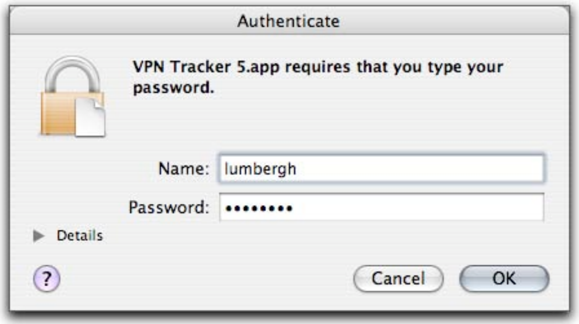


Enter the decryption password to import the bundled connection:

••••••••••••••••••••

- Enter the decryption password

VPN Tracker will now ask for an administrator password to complete the installation.



Authenticate

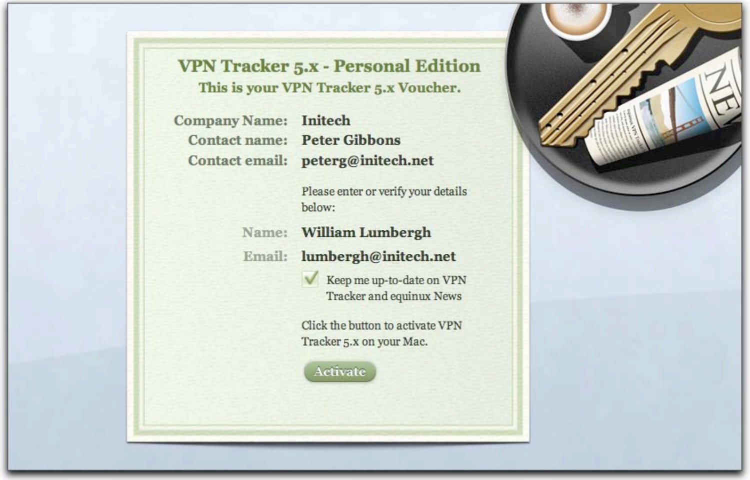
VPN Tracker 5.app requires that you type your password.

Name: lumbergh

Password: ••••••••

- Enter a local administrator username and password

VPN Tracker will present your license voucher



VPN Tracker 5.x - Personal Edition

This is your VPN Tracker 5.x Voucher.

Company Name: Initech

Contact name: Peter Gibbons

Contact email: peterg@initech.net

Please enter or verify your details below:

Name: William Lumbergh

Email: lumbergh@initech.net

☑ Keep me up-to-date on VPN Tracker and equinux News

Click the button to activate VPN Tracker 5.x on your Mac.

- Click "Activate"

VPN Tracker is now licenses and configured on your Mac. Please skip ahead to "Managing and Using Connections" to learn how to use the connection(s) provided with the bundle.

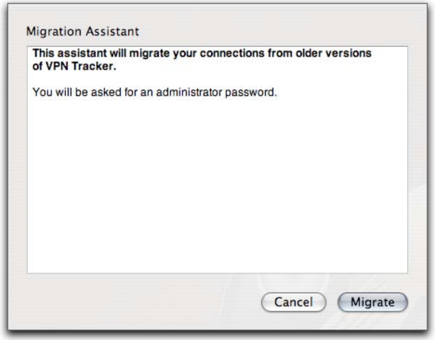
Migrating to VPN Tracker 5

Users of VPN Tracker 3 or 4 can have their existing connections migrated to the new connection profile automatically

When VPN Tracker 5 is started for the first time, it will detect existing installations of VPN Tracker 3/4 on your Mac, and scan them for connections.

To run the migration assistent manually:

- Select "File > Migrate Connections from VPN Tracker 3/4..."

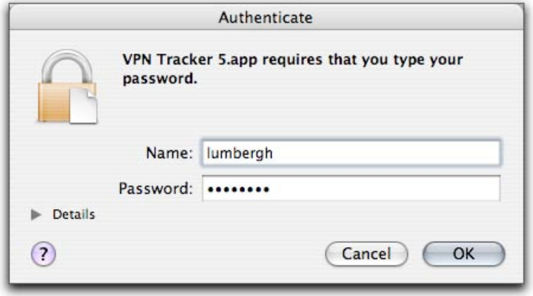


Migration Assistant

This assistant will migrate your connections from older versions of VPN Tracker.

You will be asked for an administrator password.

- Click "Migrate" in the appearing dialog window



Authenticate

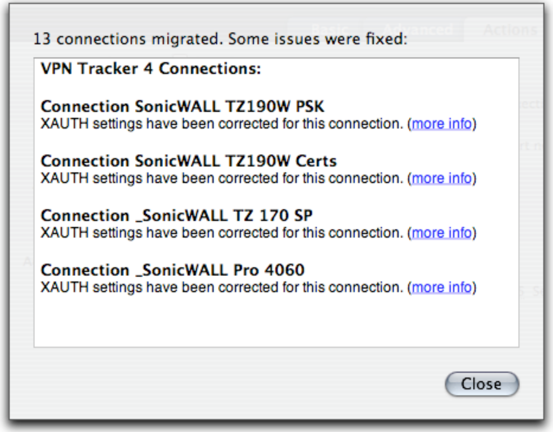
VPN Tracker 5.app requires that you type your password.

Name: lumbergh

Password: ••••••••

- Enter your administrator password
- Click "OK"

VPN Tracker will display the result, including any changes it had to apply:



13 connections migrated. Some issues were fixed:

VPN Tracker 4 Connections:

Connection SonicWALL TZ190W PSK
XAUTH settings have been corrected for this connection. (more info)

Connection SonicWALL TZ190W Certs
XAUTH settings have been corrected for this connection. (more info)

Connection _SonicWALL TZ 170 SP
XAUTH settings have been corrected for this connection. (more info)

Connection _SonicWALL Pro 4060
XAUTH settings have been corrected for this connection. (more info)

That's all – please skip ahead to "Managing and Using Connections" to learn how to use the migrated connections.

Getting Started

This chapter explains how to configure and establish a VPN connection quickly. Let's get started!

Prerequisites

To configure a VPN connection to your office (or to some other location), you will need

- A Mac (which runs VPN Tracker Professional or Personal)
- A VPN gateway at your office (at your target location)

With VPN Tracker Player, you cannot configure your own connection. In this case, you need to receive either a deployment bundle or a configuration profile from your network administrator.

When using VPN Tracker Player, please do the following:

- For instructions on installing a deployment bundle, please read "Installing a Deployment Bundle".
- For details on importing connection profiles, please skip ahead to "Assisted Setup".

If you have a license for VPN Tracker Professional or Personal, please read on.

To create a new connection:

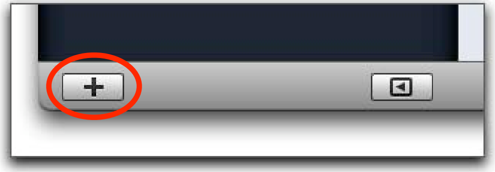
- Select "File > New Connection"

or

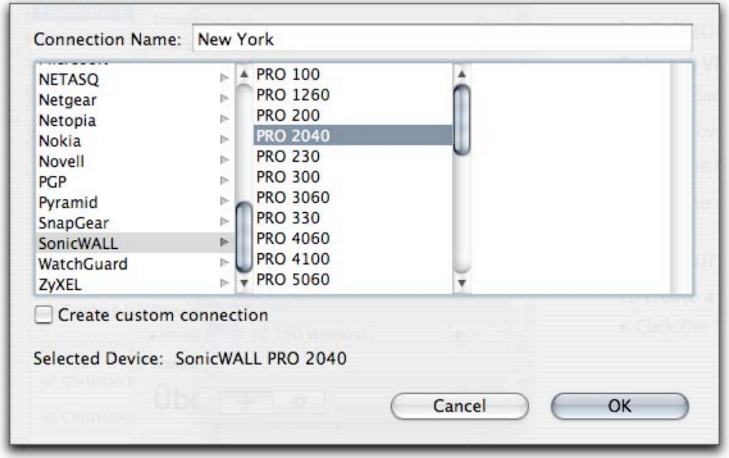
- Press ⌘-N

or

- Click the "+" button in VPN Tracker's main window



A dialog window will open.



Connection Name: New York

NETASQ	PRO 100
Netgear	PRO 1260
Netopia	PRO 200
Nokia	PRO 2040
Novell	PRO 230
PGP	PRO 300
Pyramid	PRO 3060
SnapGear	PRO 330
SonicWALL	PRO 4060
WatchGuard	PRO 4100
ZyXEL	PRO 5060

□ Create custom connection

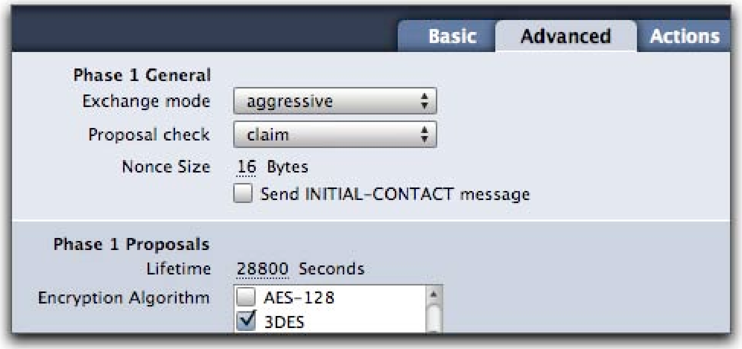
Selected Device: SonicWALL PRO 2040

- Select your preferred connection name
- Select the vendor and device name of your VPN gateway
- Enter a connection name

- Click “OK”

The connection will be created, and the main window will extend to display the configuration options.

When you selected a device, this device’s standard profile was automatically applied to your connection. The profile collects a couple of general VPN settings (as opposed to the connection-specific settings which are configured individually). These settings can be found on the “Advanced“ tab in VPN Tracker’s main window.



Phase 1 General

Exchange mode: aggressive

Proposal check: claim

Nonce Size: 16 Bytes

☐ Send INITIAL-CONTACT message

Phase 1 Proposals

Lifetime: 28800 Seconds

Encryption Algorithm: ☐ AES-128 ☑ 3DES

If you just installed the gateway yourself, and did not touch its VPN-related settings, you should not need to change anything under “Advanced“ in VPN Tracker either.

Note If you or your network administrator changed the default VPN settings of the device, you will have to modify the “Advanced“ settings in VPN Tracker. Please refer to the VPN Tracker manual (”Modifying a Device Profile“) for further information.

Setting Up the VPN Gateway

If you don’t have a VPN gateway already, a list of VPN gateways which have been tested with VPN Tracker can be found at http://www.equinux.com/vpntracker/interop.

If you’re new to networking, here are some basic configuration hints. The VPN gateway should be connected to the Internet directly (i.e. the gateway should be directly connected to a DSL modem or similar). It is possible to place the VPN gateway behind another firewall or router, but this setup is more complex.

The VPN gateway needs to be the default gateway for all other computers to be accessed through the VPN tunnel. For Macs, this means that the gateway’s local interface address is stored under System Preferences > Network > TCP/IP > Router.

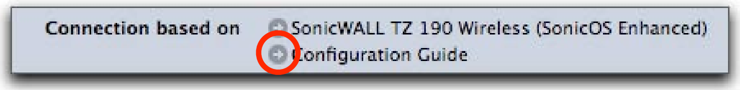
The gateway should also have a static public IP address, which is usually available from Internet providers as a paid option. If this option is not available, you can also register a dynamic hostname for free at services like DynDNS. A dynamic hostname requires that your VPN gateway supports automatic updates of its current IP address with the dynamic hostname service.

Please refer to your gateway's manual for more detailed instructions.

Configuration Guide

For the VPN configuration of your gateway, please refer to the device's configuration guide:

- Click the "Configuration Guide" link next to the device name in the "Basic" tab



Connection based on SonicWALL TZ 190 Wireless (SonicOS Enhanced)
Configuration Guide

The guide will show you how to configure both the gateway and VPN Tracker, and how to establish the connection afterwards.

Note Configuring connections is not possible with VPN Tracker Player.

When you're done with setting up a connection, please skip ahead to "Managing and Using Connections".

No Device Profile?

If your VPN gateway is not available in VPN Tracker, we have not tested it yet, and cannot provide a configuration guide or support.

However, if the device supports the IPSec standard, it is likely to work with VPN Tracker.

To configure an untested device:

- Please refer to "Custom Devices"

No Gateway Access?

If you cannot configure the VPN gateway yourself:

- Please read the chapter ("Assisted Setup")

Assisted Setup

If you don't have access to the VPN gateway yourself, you depend on the help of your IT department to configure a connection.

Using a Deployment Bundle

Ideally, your IT department will provide a deployment bundle which makes installing, activating and configuring a one-step process. Please refer to "Installing a Deployment Bundle" for details.

Instructions on how to create deployment bundles can be found in "Exporting Connections".

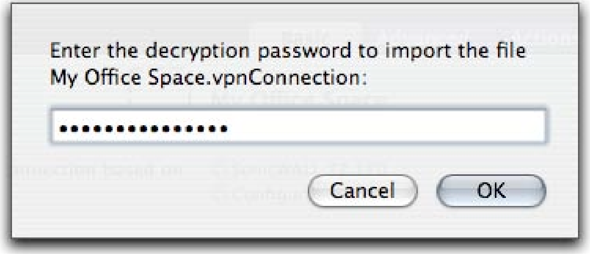
Importing a Connection Profile

In many cases, your IT department will provide a VPN Tracker profile for you to import. Such a profile can be exported from VPN Tracker Professional, as described in "Exporting Connections".

To import a connection profile:

- Double-click the connection file

You will be asked for a decryption password. This password is set (and revealed to you) by your network administrator. It is set specifically for the connection profile, and is not necessarily identical to your normal login password for company network services (see the "IPSec Explained: Authentication" section in this manual).


Enter the decryption password to import the file My Office Space.vpnConnection:

•••••••••••••••

- Enter the decryption password provided by your IT department

That's it. The new connection will appear in your connection list. Please skip ahead to "Managing and Using Connections".

Manual Configuration

If your company's IT department is not Mac-based, you will usually get information such as a pre-shared key, the VPN gateway address and a pointer to a Windows-based VPN client.

To connect to your office using VPN Tracker, you need to obtain at least the following:

- The vendor and model name of the VPN gateway
- A pre-shared key (or certificates)
- The VPN gateway address

In many cases, you will also need

- The remote network

- An XAUTH username and password
- Local and remote identifiers

If the gateway's basic VPN configuration (factory defaults) has not been altered, this should suffice to create a working connection. Please see ″Getting Started“, above, and the configuration guide for the respective device for details.

If the gateway is not listed in VPN Tracker's device list, please read "Creating a Custom Connection".

Terminology

Your network administrator might use a different VPN terminology and cannot tell you where to put the connection-specific settings in VPN Tracker.

To avoid any confusion:

- Please open the configuration guide for the device (if there is a guide for VPN Tracker 5)
- See "Appendix: Terminology"

Managing and Using Connections

Your VPN connection is configured, so the next step is obvious: Start using it!

Some of the features described in this chapter are only available in VPN Tracker Personal or Pro.

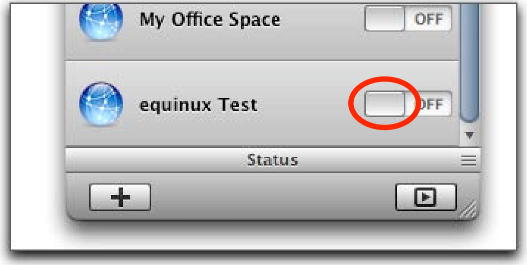
Starting a Connection

To start a connection:

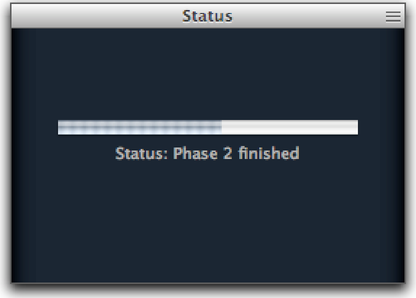
- Click the start slider next to the connection

or

- Drag the slider to the right

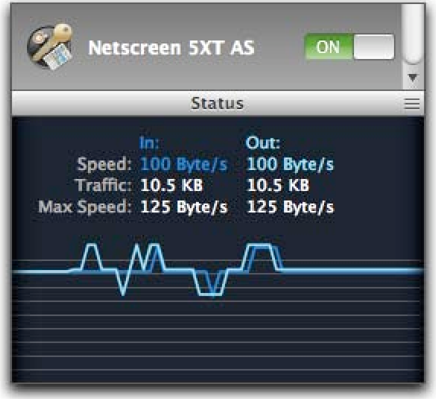


While the connections is being established, the status area below the connection list will show the progress.



Status: Phase 2 finished

After some seconds, the green "ON" status will be displayed. You're connected!



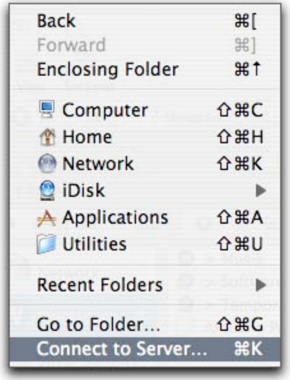
```
             In:             Out:
Speed:       100 Byte/s      100 Byte/s
Traffic:     10.5 KB         10.5 KB
Max Speed:   125 Byte/s      125 Byte/s
```

Once the connection is up, the status area will display some data about the performance, such as current speed, transferred data and maximum speed.

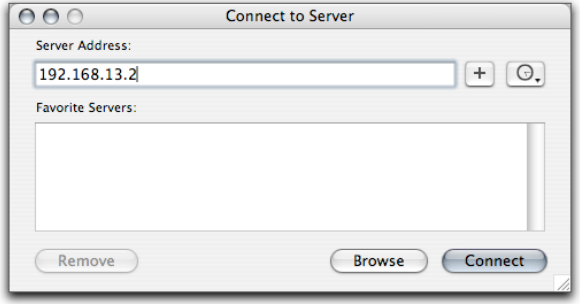
Accessing Files

To access files in your Private Network, just follow the steps below:

- In the Finder, select “Go > Connect To Server...”



- Enter the IP address of the machine you want to connect to


Connect to Server

Server Address: 192.168.13.2

Favorite Servers:

- Click “Connect”

- Enter your username and password to access a folder on the server

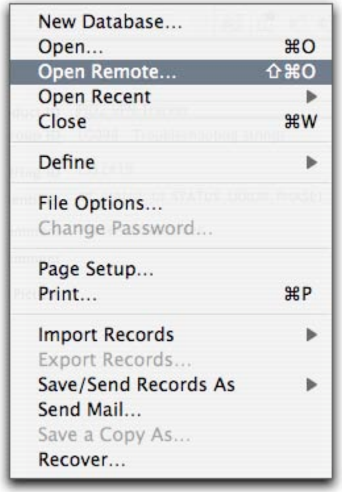
Note When connecting to a Windows fileserver, the IP address needs to be prefixed with “smb://”.

Accessing a FileMaker Database

To access a database available in your Private Network, just follow the steps below:

- Start the FileMaker application

- In FileMaker, select “File > Open Remote...“



- Click “Add“

- Enter the IP address of the FileMaker server
- Enter the Favorite Host's name for this machine
- Click "Save"
- Select a database from the list of Available Files and click "Open"

You're now able to access your FileMaker databases as usual.

Restarting a Connection

Sometimes, you might need to restart a running connection for some reason (e.g. to obtain a new DHCP lease, or because the tunnel expired on the gateway).

To restart a connection:

- Select the connection
- Choose "Connection > Restart"

or

- Right-click the connection
- Select "Restart Connection" from the contextual menu

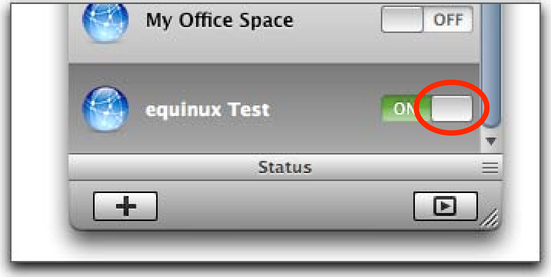
Stopping a Connection

To stop a connection:

- Click the stop button next to the connection

or

- Drag the slider to the left



Managing Connections

If you're an admin working with many connections, VPN Tracker offers many convenient features for managing connections.

To rename, duplicate or delete a connection:

- Select the connection
- Choose the appropriate option from the "Connection" menu

or

- Right-click the connection
- Select the desired option from the contextual menu

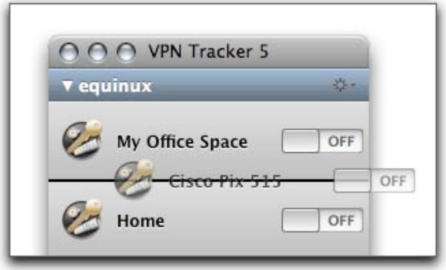
Modifying Connection Settings

Manual creation of a connection is described in "Creating a Custom Connection". Please refer to that section for detailed instructions.

Reordering the Connection List

To reorder the connection list:

- Click and hold a connection
- Drag it to the desired position
- Release the mouse button

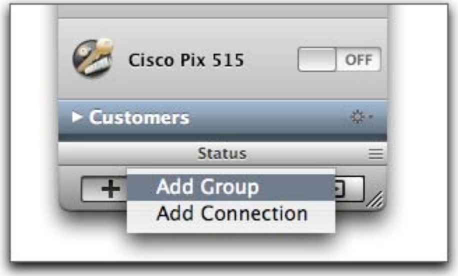


Connection Groups

In VPN Tracker Personal and Pro, connections can be organized in groups.

To create a group:

- Click and hold the plus button in the Connection Viewer
- Select “Add Group”



or

- Select “File > New Group”

or

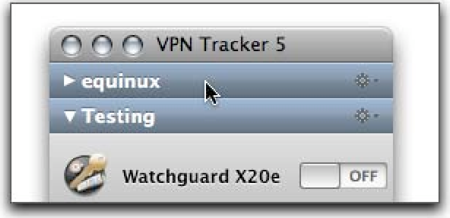
- Press ⌘-⌥-N
- Enter a name for your group
- Press Return

Moving connections into a group works just like reordering the connection list (see above).

Groups can be opened and closed to keep your connection list tidy.

To open or close a group:

- Click the group bar

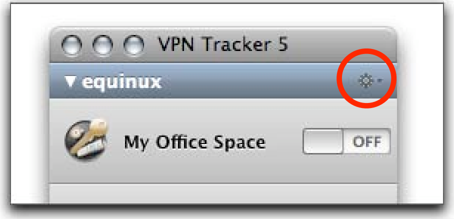


The triangle to the left will change its state, and all connections within the group will be hidden (or shown).

Each group has a contextual menu accessible through the gear symbol at the right of the group bar. It can be used to

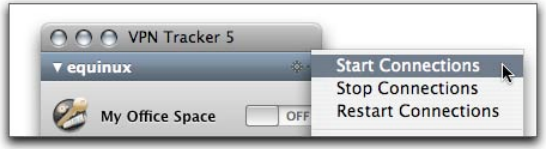
start, stop or restart all connections in a group

rename, duplicate or delete a group



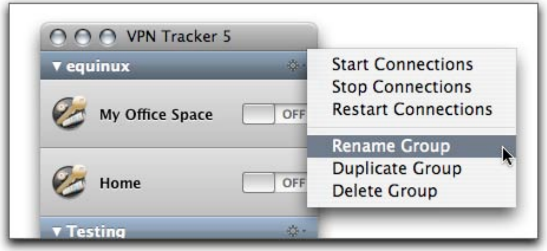
To start, stop or restart all connections in a group:

- Click and hold the gear symbol
- Select the desired option



To rename, duplicate or delete a group:

- Click and hold the gear symbol
- Select the desired option



Actions

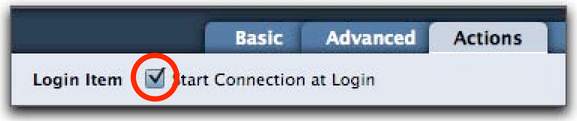
VPN Tracker 5 can start and stop based on your current location or network environment, or execute specified tasks after establishing or before stopping a connection.

Automatic Startup

Each connection can be started , so it will start automatically when you log in to your Mac. This is quite useful for desktop machines using VPN connection(s) to offices or central databases all the time.

To activate automatic startup for a connection:

- Select the connection
- Switch to the "Actions" tab



Login Item ☑ Start Connection at Login

- Check the box "Start Connection at Login"

Location Awareness

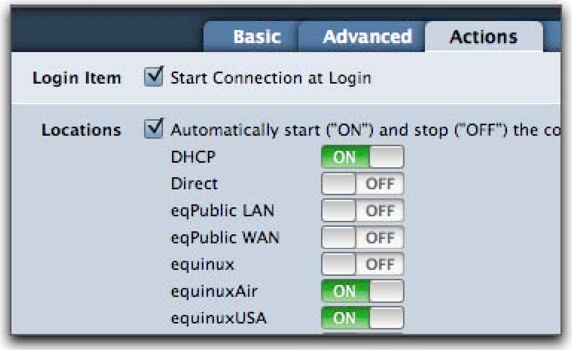
VPN Tracker 5 offers two variants of location awareness. It will detect

- Manual location changes
- Switches to or from certain AirPort networks

For each location defined in your Mac's System Preferences, you can explicitly activate or deactivate a connection.

To activate a connection for a location:

- Select the connection
- Switch to the "Actions" tab



Login Item ☑ Start Connection at Login

Locations ☑ Automatically start ("ON") and stop ("OFF") the co

DHCP	ON
Direct	OFF
eqPublic LAN	OFF
eqPublic WAN	OFF
equinux	OFF
equinuxAir	ON
equinuxUSA	ON

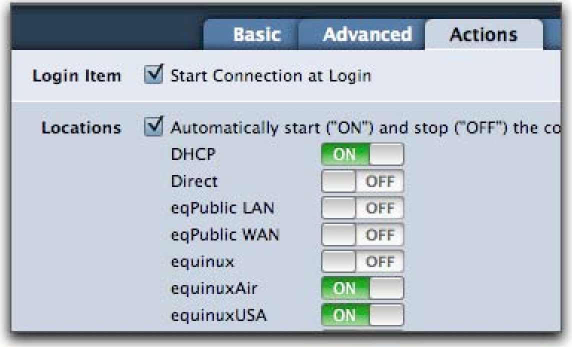
- Drag the slider for the location to the right

or

- Click the slider (if the connection was deactivated before)

To deactivate a connection for a location:

- Select the connection
- Switch to the "Actions" tab



Login Item ☑ Start Connection at Login

Locations ☑ Automatically start ("ON") and stop ("OFF") the co

DHCP	ON
Direct	OFF
eqPublic LAN	OFF
eqPublic WAN	OFF
equinux	OFF
equinuxAir	ON
equinuxUSA	ON

- Drag the slider for the location to the left

or

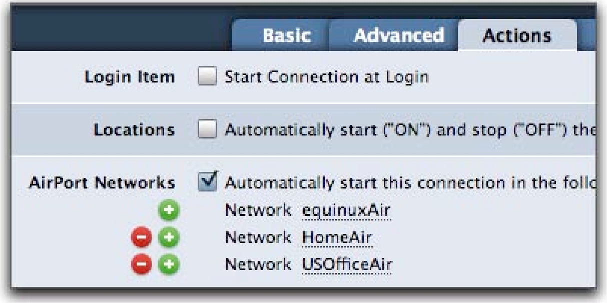
- Click the slider (if the connection was activated before)

Switches between different AirPort networks (within the same location) are handled differently.

You can instruct VPN Tracker to start (or restart) a connection when a certain AirPort network becomes the primary interface.

To start (or restart) a connection automatically for an AirPort network:

- Select the connection
- Switch to the "Actions" tab
- Click the green "+" symbol (if you need to add an additional AirPort network)
- Enter the network's SSID



Login Item □ Start Connection at Login

Locations □ Automatically start ("ON") and stop ("OFF") the

AirPort Networks ☑ Automatically start this connection in the follo

Network equinuxAir

Network HomeAir

Network USOfficeAir

Note If an AirPort network is not part of the list, the VPN connection will simply drop when the primary network interface is changed.

To remove an Airport network from the list:

- Click the red "-" symbol next to it

VPN Startup and Shutdown Actions

Older versions of VPN Tracker let you place UNIX scripts in a certain folder to execute them based on the current connection status.

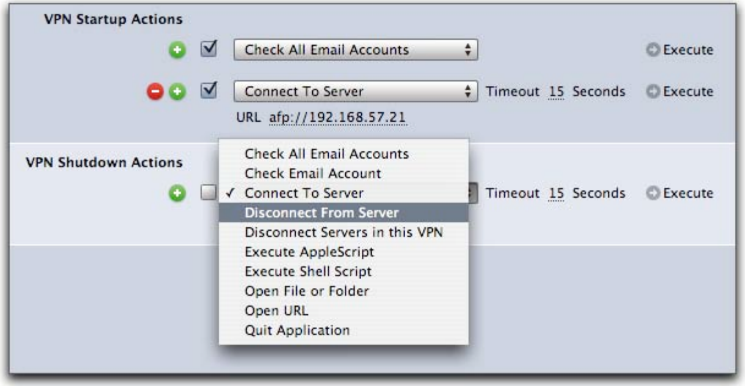
Note Startup and Shutdown Actions will only be executed when a connection is started or stopped manually.

VPN Tracker 5 integrates this concept into the user interface, so you don't have to be familiar with UNIX scripting to automate common tasks.

> **TIP** If you're using VPN Tracker Professional, you can even export a set of actions with your connection.

To create a new VPN startup or shutdown action:

- Click the green "+" symbol next to an existing entry
- Select the desired action
- Provide login details or a file path (if applicable)



VPN Startup Actions

☑ Check All Email Accounts

☑ Connect To Server Timeout 15 Seconds

URL afp://192.168.57.21

VPN Shutdown Actions

□ Timeout 15 Seconds

Actions can be deleleted or deactivated temporarily.

To deactivate an action:

- Uncheck the box next to it

To delete an action:

- Click the red "-" symbol next to it

Device Profiles

VPN Tracker comes equipped with more than 250 device profiles to simplify the configuration of VPN connections. This chapter explains how to handle profiles.

Whenever you create a new connection, you're asked to select a device. Each device profile in the list is linked to a set of parameters based on the factory default of the respective device. Selecting a device is equivalent to configuring a set of basic parameters in the Basic and Advanced tab of your connection.

Modifying Default Settings

If your gateway is listed in VPN Tracker, but you or your network administrator changed its VPN-related default settings (e.g. to enforce high-security encryption), you will need to modify these settings in VPN Tracker, too.

Note The settings stored in a device profile are **copied** to your connection when a device is selected. Modifying them in the connection will **not** affect the device profile.

Please do the following:

- Create a connection as described in "Getting Started"
- Locate the relevant options in VPN Tracker
- Change them to match the new settings on the gateway

TIP In most cases, the changes affect the proposals (Phase 1 and/or Phase 2) accepted by the gateway. These can be found in the "Advanced" tab of your connection.

Selecting a Different Device

Instead of modifying settings manually, you can also revise your device selection. This will overwrite most of your connection parameters using the values stored in the device profile.

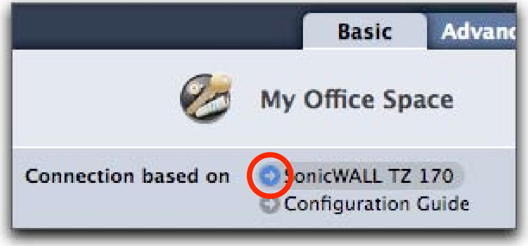
The following parameters are **not** overwritten:

- VPN gateway address
- Topology
- Remote address or network(s)
- Local address or network(s)
- Identifiers (type and value)
- XAUTH
- Client Provisioning

- DNS

To select a different device:

- Switch to the "Basic" tab of your connection
- Click the arrow next to the device name



Connection based on SonicWALL TZ 170 Configuration Guide

- Select a device
- Click "OK"

Creating a Custom Connection

If your VPN gateway is not listed in VPN Tracker, and it is not known to behave similarly to another device on the list, you can create a custom connection.

While you could also modify a connection based on an existing device profile, creating a custom connection is the preferred option for unknown devices. Device profiles intentionally hide options known to be unsupported by the corresponding device. Only custom connections will give you full access to all options available in VPN Tracker.

We will assume that the gateway has been configured already. Please note that all settings configured in VPN Tracker have to match the corresponding settings on the gateway.

Note Technical details on all options mentioned in this section can be found in "IPSec Explained".

To create a custom connection:

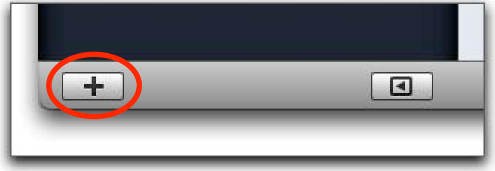
- Select "File > New Connection"

or

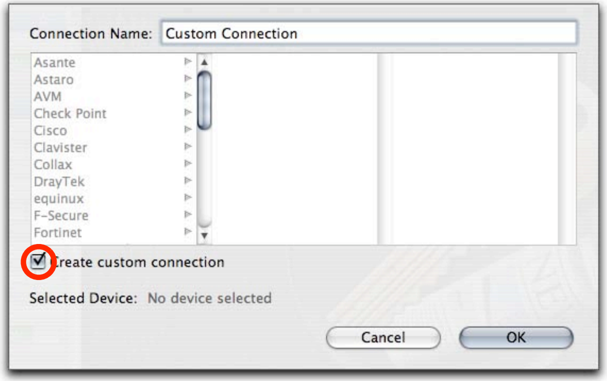
- Press ⌘-N

or

- Click the "+" button in VPN Tracker's main window



- In the device chooser dialog, check "Create custom connection"



Connection Name: Custom Connection

☑ Create custom connection

Selected Device: No device selected

- Enter a name for your connection
- Click "OK"

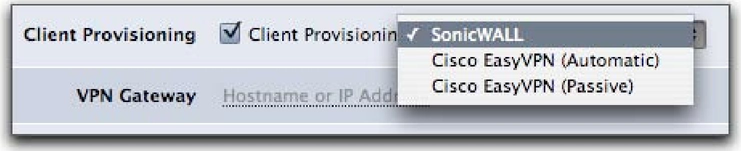
You should configure the basic settings first.

Client Provisioning

Some gateways support automatic configuration of certain parameters (like the local address, the remote network or DNS settings).

If your VPN gateway is configured to use Client Provisioning:

- Check the Client Provisioning box
- Select the desired Client Provisioning type

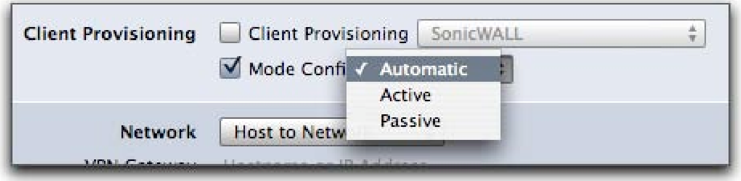


Client Provisioning ☑ Client Provisionin ✓ SonicWALL

VPN Gateway Hostname or IP Addr

If your VPN gateway is configured to use Mode Config:

- Check the Mode Config box
- Select the desired Mode Config type



Client Provisioning □ Client Provisioning SonicWALL

☑ Mode Confi ✓ Automatic

Network Host to Netw

Note When using either Client Provisioning or Mode Config, the parameters sent by the gateway cannot be specified manually.

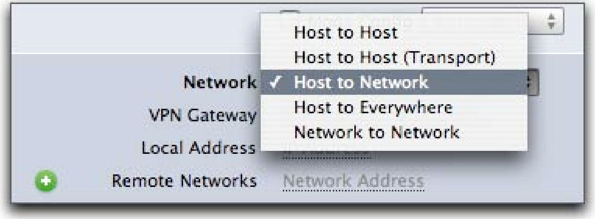
Network

A connection can be configured for different network topologies:

- **Host to Host** connects your Mac to a single remote computer. You can select tunnel or transport mode, where tunnel mode is recommended for most environments.
- **Host to Network** connects your Mac to a remote network. This is the most commonly used topology.
- **Host to Everywhere** will send all your network traffic through the tunnel. This mode is recommended for securing

AirPort connections (e.g. in a public WLAN), but it is not supported by all devices.

- **Network to Network** established a connection to a remote network and turns your Mac into the VPN gateway for the local network. This topology is only available in VPN Tracker Professional.



After selecting a topology, the **VPN gateway** has to be specified. This is the public IP address (or hostname) of the gateway you intend to connect to.

You can also choose a **Local Address** for the connection. This is the virtual IP address under which your Mac will be seen in the remote network. For most connections, this setting is optional. When using Client Provisioning or Mode Config, it is not available.

The **Remote Network(s)** are the networks you would like to access through the VPN tunnel. This setting is hidden when using the "Host to Everywhere", or when using complete Client Provisioning.

To configure your network settings:

- Select the desired topology
- Enter the VPN gateway address
- Enter a local address (if applicable)
- Enter one or more remote network(s) (if applicable)

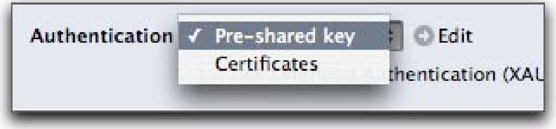
Authentication

Before establishing the VPN tunnel, both partners need to authenticate using either a pre-shared key (aka group password), or certificates. While pre-shared keys are the most convenient authentication method, certificates offer additional security.

In addition to standard authentication, VPN Tracker supports **Extended Authentication (XAUTH)** to enforce individual authentication for each VPN client connecting to the gateway.

To configure authentication:

- Select an authentication method

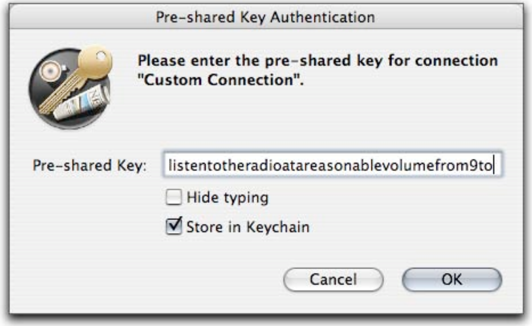


- Click "Edit" to enter the pre-shared key or to edit the certificates used for this connection

or

- Right-click the connection
- Choose "Edit Pre-Shared Key" from the contextual menu (note that you cannot use this method to select certificates)

- Check "Store in Keychain" if you don't want to enter the pre-shared key manually each time you establish the connection



Pre-shared Key Authentication

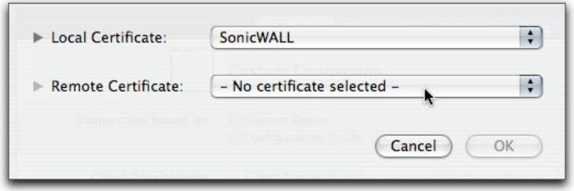
Please enter the pre-shared key for connection "Custom Connection".

Pre-shared Key: listentotheradioatareasonablevolumefrom9to

□ Hide typing

☑ Store in Keychain

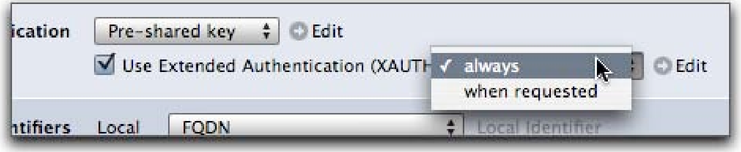
- When editing certificates, please select a local and a remote certificate for this connection



Local Certificate: SonicWALL

Remote Certificate: – No certificate selected –

- Click "OK"



ication Pre-shared key

☑ Use Extended Authentication (XAUTH ✓ always

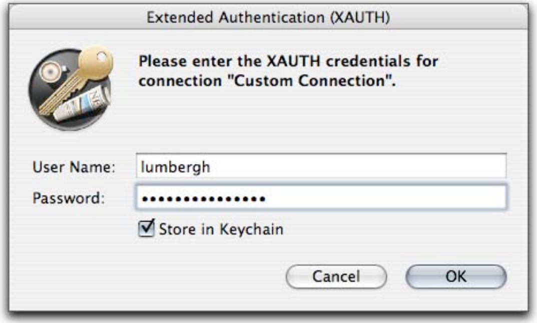
ntifiers Local FQDN

If your gateway requires Extended Authentication (XAUTH):

- Check the XAUTH box, if applicable
- Select the XAUTH type (usually always)
- Click "Edit"

or

- Right-click the connection
- Choose "Edit XAUTH Credentials" from the contextual menu



Extended Authentication (XAUTH)

Please enter the XAUTH credentials for connection "Custom Connection".

User Name: lumbergh

Password: •••••••••••••••

☑ Store in Keychain

- Enter your user name and password

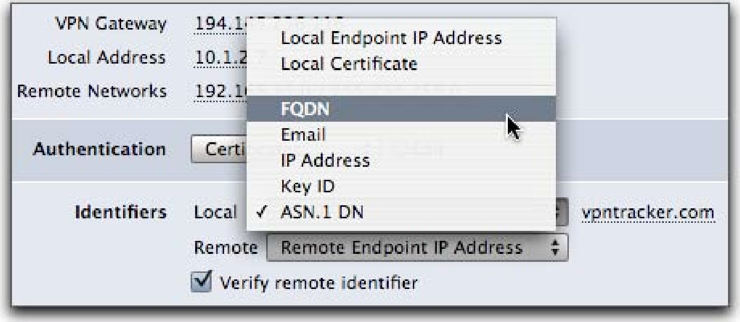
Identifiers

The identifiers are used to identify the VPN peers during the first phase of the tunnel establishment, and to select the appropriate IPSec configuration. For both the local and the remote identifier, you need to specify both a type and a value.

To configure identifiers for your connection:

- Select a type from the pop-up menu for the local identifier
- Enter a value (if applicable)
- Select a type from the pop-up menu for the remote identifier

- Enter a value (if applicable



VPN Gateway 194.1

Local Address 10.1.2

Remote Networks 192.1

Authentication Certi

Identifiers Local ✓ ASN.1 DN vpntracker.com

Remote Remote Endpoint IP Address

☑ Verify remote identifier

- Check "Verify remote identifier" to enforce verification of the remote identifier

DNS

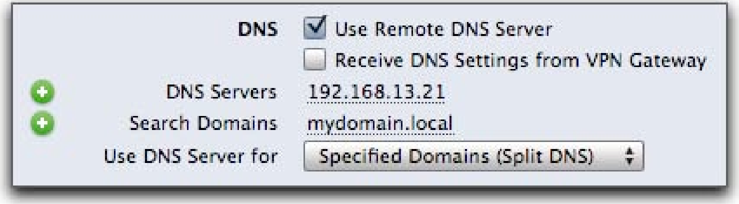
A VPN tunnel can be configured to use a remote DNS server (so your Mac can resolve hostnames from the remote network).

To enable remote DNS:

Check the box next to "Use Remote DNS Server"

When using Client Provisioning or Mode Config, you can choose to receive DNS settings from the VPN gateway.

Check "Receive DNS Settings..." if applicable



DNS ☑ Use Remote DNS Server

□ Receive DNS Settings from VPN Gateway

DNS Servers 192.168.13.21

Search Domains mydomain.local

Use DNS Server for Specified Domains (Split DNS)

- Enter a DNS server's IP address
- Enter a search domain (optional)
- Choose between Split DNS and Global DNS

Split DNS will use the remote DNS server only for the search domains specified before, while Global DNS will use it for all domains.

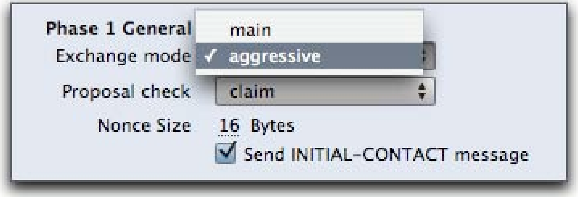
Note Global DNS will work only when the remote DNS server can resolve public hostnames (like google.com) directly or indirectly.

Advanced Settings

The "Advanced" tab contains general settings which are usually device-specific, but not connection-specific (although you can configure connections . encryption and authentication settings. When using a device profile without any modifications, you usually don't have to visit this tab.

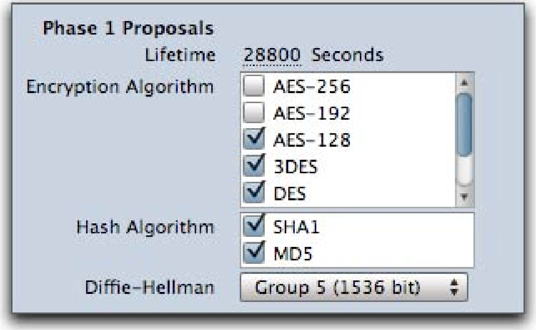
For custom devices, VPN Tracker preselects a standard set of proposals etc. We will highlight only the parameters which require special attention.

- The **exchange mode** for Phase 1 is either “main” or “aggressive”



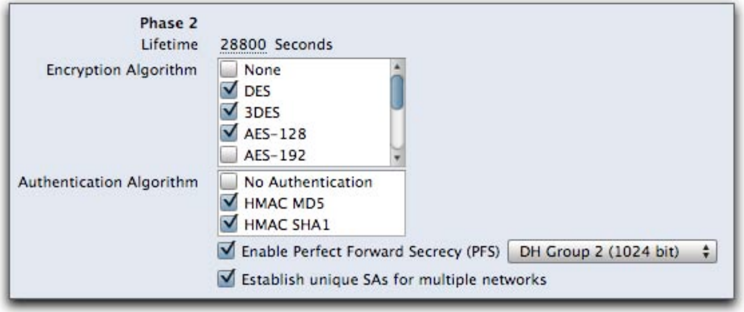
Phase 1 General
Exchange mode: main / ✓ aggressive
Proposal check: claim
Nonce Size: 16 Bytes
☑ Send INITIAL-CONTACT message

- There needs to be at least one set of matching **proposals** (combination of encryption, hash algorithm and Diffie-Hellman group) for Phase 1 between the gateway and VPN Tracker.



Phase 1 Proposals
Lifetime: 28800 Seconds
Encryption Algorithm: □ AES-256, □ AES-192, ☑ AES-128, ☑ 3DES, ☑ DES
Hash Algorithm: ☑ SHA1, ☑ MD5
Diffie-Hellman: Group 5 (1536 bit)

- For Phase 2, the requirement is the same. If a Diffie-Hellman group is specified for Phase 2 on the gateway, please make sure to enable **Perfect Forward Secrecy (PFS)**



Phase 2
Lifetime: 28800 Seconds
Encryption Algorithm: □ None, ☑ DES, ☑ 3DES, ☑ AES-128, □ AES-192
Authentication Algorithm: □ No Authentication, ☑ HMAC MD5, ☑ HMAC SHA1
☑ Enable Perfect Forward Secrecy (PFS): DH Group 2 (1024 bit)
☑ Establish unique SAs for multiple networks

Note It is usually safe to select multiple algorithms, but some devices stop responding when being sent more than one proposal

- Synchronize the **lifetimes** for both Phase 1 and Phase 2 with the gateway. Lifetime differences might not prevent a tunnel from being established, but they will cause problems when negotiating new keys (re-keying)

For the other advanced settings, there’s a general rule: If you don’t know them, don’t touch them. You might have to edit them when your custom connection fails, but it is recommended to try connecting with the defaults first.

Deployment

As an admin, you probably don't want to configure each user's Mac manually. VPN Tracker Professional lets you export connections or even complete deployment images.

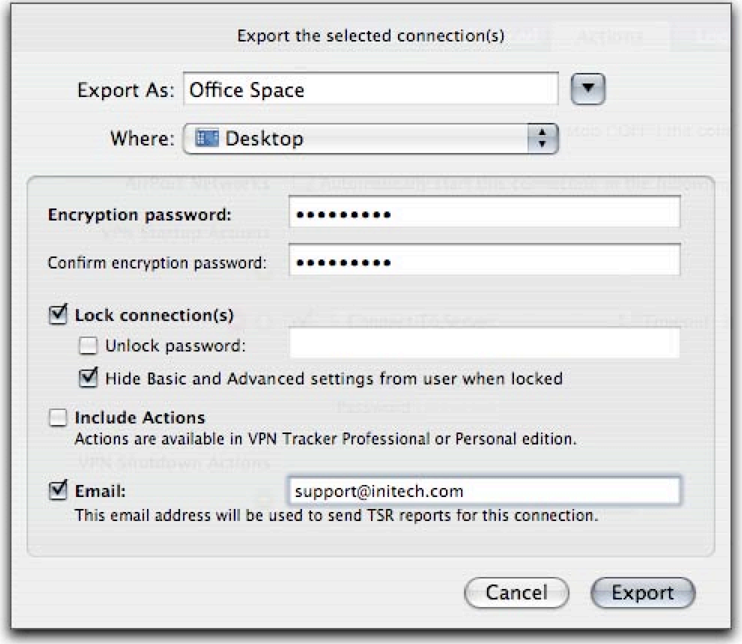
Exporting Connections

Older version of VPN Tracker Professional offered an export function that would create encrypted connection files. VPN Tracker 5 Professional offers several new options when exporting connections.

A connection file can now contain one or more connections, which makes it much easier to distribute a complete set of connections.

To export connections:

- Select one or more connections
- Select "File > Export Connection..."
- Provide an encryption password
- Select your preferred options for the connection file (s. below)
- Click "Export"



Export the selected connection(s)

Export As: Office Space

Where: Desktop

Encryption password: ••••••••••

Confirm encryption password: ••••••••••

☑ Lock connection(s)

□ Unlock password:

☑ Hide Basic and Advanced settings from user when locked

□ Include Actions
Actions are available in VPN Tracker Professional or Personal edition.

☑ Email: support@initech.com
This email address will be used to send TSR reports for this connection.

Locking Connections

As an administrator you probably don't want all your users to know about the pre-shared key of your company's VPN connection, and you certainly don't want them to edit the connection settings. By locking a connection, you can effectively prevent any user from seeing sensitive information and from damaging his or her VPN access.

To create a locked connection:

- Check the "Lock connection(s)" box when exporting connections

You might want to allow certain users to know about the settings. This is what the unlock password is for – if you send the encryption and the unlock password with a locked connection file, the recipient will be able to see (and edit) the settings.

Note It is highly recommended to choose different passwords for encrypting and locking the connection file, but this is not enforced by VPN Tracker.

To specify an unlock password:

- Check the "Unlock password" box
- Enter an unlock password

For increased security, you can even hide all the settings (including the gateway address) from the users.

To hide all settings for a connection:

- Check the "Hide Basic and Advanced settings..." box

Note This setting only applies to a locked connection. If a user has access to an unlock password, he/she can view all settings.

Deployment Bundles

To install VPN Tracker for a large number of clients, there's an even easier way to distribute VPN Tracker.

The application lets you create bundles (in DMG format) containing a license, connection profiles and the application itself. This bundle makes the installation process quite simple (see "Installing a Deployment Bundle").

To prepare deployment:

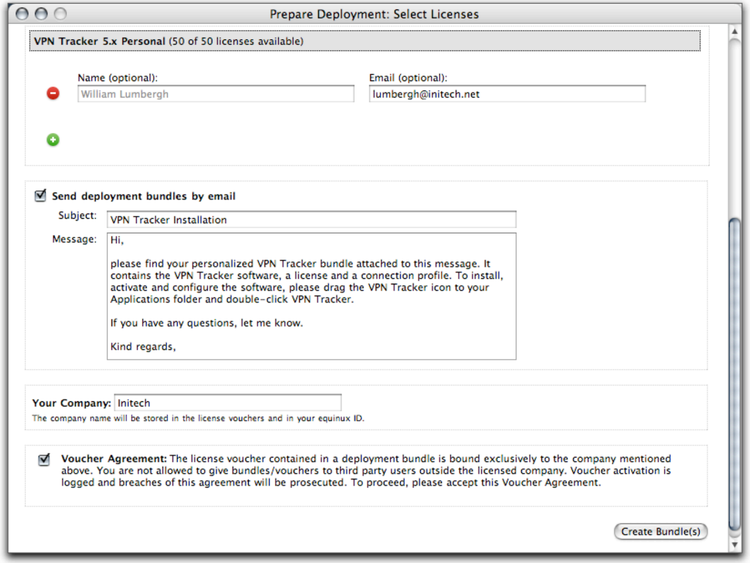
- Select one or more connections
- Select "File > Prepare Deployment..."

The dialog for exporting connections will appear. Please follow the instructions for exporting connections above. After clicking "OK", VPN Tracker will connect to the equinux licensing server.

- Login with your equinux ID and password
- Click the green "+" symbol to add unused licenses to the deployment cycle
- Enter your company name
- Read and accept the Voucher Agreement by checking the box next to it

If you want to send the deployment bundles using Apple Mail:

- Check the appropriate box
- Make sure to specify an email address for each bundle/voucher
- Modify the mail subject and message



Prepare Deployment: Select Licenses

VPN Tracker 5.x Personal (50 of 50 licenses available)

Name (optional): William Lumbergh

Email (optional): lumbergh@initech.net

☑ **Send deployment bundles by email**

Subject: VPN Tracker Installation

Message: Hi,

please find your personalized VPN Tracker bundle attached to this message. It contains the VPN Tracker software, a license and a connection profile. To install, activate and configure the software, please drag the VPN Tracker icon to your Applications folder and double-click VPN Tracker.

If you have any questions, let me know.

Kind regards,

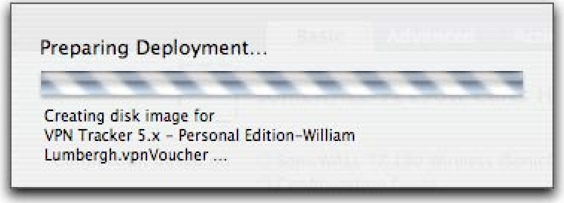
Your Company: Initech

The company name will be stored in the license vouchers and in your equinux ID.

☑ **Voucher Agreement:** The license voucher contained in a deployment bundle is bound exclusively to the company mentioned above. You are not allowed to give bundles/vouchers to third party users outside the licensed company. Voucher activation is logged and breaches of this agreement will be prosecuted. To proceed, please accept this Voucher Agreement.

- Click "Create Bundle(s)"

VPN Tracker will start creating the deployment bundle(s).



Preparing Deployment…

Creating disk image for
VPN Tracker 5.x - Personal Edition-William
Lumbergh.vpnVoucher …

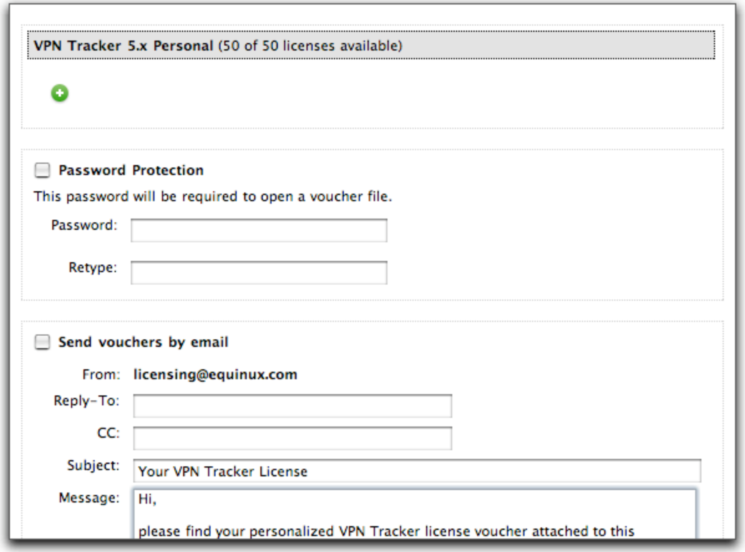
All bundles will be stored on your harddisk. If the email option was checked, it will also create email messages (one per bundle/voucher) in Apple Mail.

Distributing Licenses

If you only need to distribute licenses, you can do so using our license manager.

To distribute license vouchers for VPN Tracker:

- Open https://www.equinux.com/eqnetwork/licensemanager/issue_voucher.html
- Login with your equinux ID and password
- Click the green "+" symbol to add unused licenses to the deployment cycle



VPN Tracker 5.x Personal (50 of 50 licenses available)

□ **Password Protection**

This password will be required to open a voucher file.

Password:

Retype:

□ **Send vouchers by email**

From: **licensing@equinux.com**

Reply-To:

CC:

Subject: Your VPN Tracker License

Message: Hi,

please find your personalized VPN Tracker license voucher attached to this

- Check the “Password Protection” box (this is not required, but highly recommended
- Type and retype a password

If you want the licensing server to send the mails for you:

- Check the “Send vouchers by email” box
- Make sure to specify an email address for each voucher
- Specify a reply-to address (so users can contact you if something goes wrong)
- Modify the mail subject and message
- Click “Create Voucher(s)”

The vouchers will automatically be stored on your harddisk. If the email option was checked, each user will be sent a message from licensing@equinux.com with his/her voucher as an attachment.

Troubleshooting

Sometimes, your connection might not work as expected.

There are two major issues which can keep a connection from being established: incorrect configuration and local routers not compatible with VPN traffic.

Before contacting your network administrator or equinux technical support, please take a look at the connection's log file.

Known Limitations

There are some limitations of a VPN connection compared to a direct connection to a Private Network.

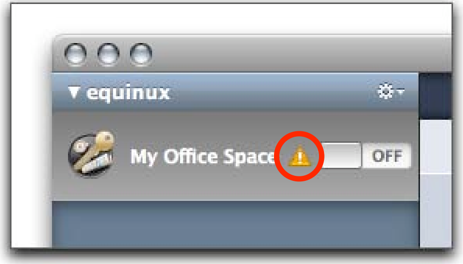
- **Bonjour**: As Bonjour Chat is not supported over a VPN tunnel, you'll need to use iChat server in order to chat remotely.
- **Browsing the network**: You can't "browse" the remote network as you're normally used to. You need to connect to each machine manually, using its IP address or hostname.

These limitations are not bugs, but inherent to the technologies involved.

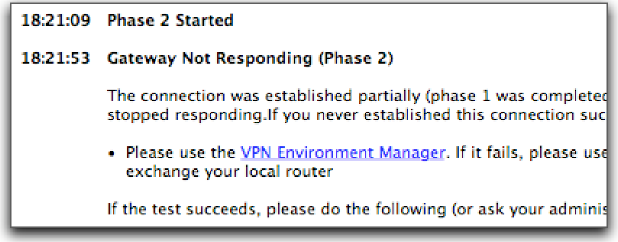
Connection Log

Please do the following:

- Click the yellow triangle next to the slider



VPN Tracker will display the connection log and describe in plain English what went wrong.



```
18:21:09   Phase 2 Started

18:21:53   Gateway Not Responding (Phase 2)

           The connection was established partially (phase 1 was completed
           stopped responding.If you never established this connection suc

           •  Please use the VPN Environment Manager. If it fails, please use
              exchange your local router

           If the test succeeds, please do the following (or ask your adminis
```

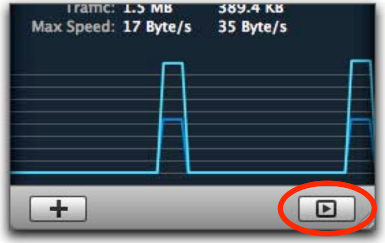
Log Levels

If you're familiar with the details of IPSec, you can also increase the log level.

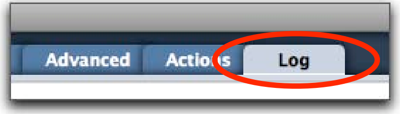
To see more information in the connection log:

- Select a connection

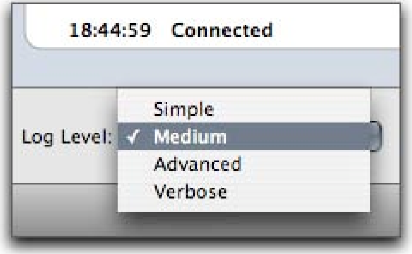
- Expand the connection list by clicking the expansion button



- Click the "Log" tab



- Switch the log level to a higher level



18:44:59 Connected

Log Level: ✓ Medium

VPN Environment Manager

In some cases, the local router will not handle VPN traffic correctly. The VPN Environment Manager analyzes the VPN capabilities of your router, and stores the results. Based on these results, VPN Tracker will pick the right communication method when connecting through this router.

To test the router, please do the following:

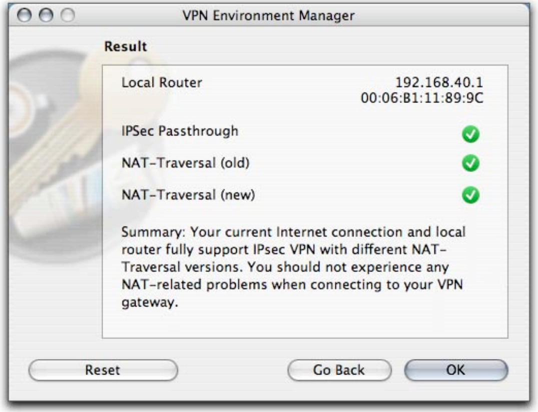
- Select "Help > VPN Environment Manager..."
- Click "Continue"

VPN Tracker now contacts a VPN gateway at equinux and tries to establish a connection. It conducts three different tests to check whether the local router supports IPSec Passthrough and/or two variants of NAT-Traversal.

> **Note** The VPN Environment Manager needs to run only once for each router (network environment).

- If all goes well, you will see three green checkmarks stating that your router is fully compatible with IPSec. The downside is that any problem you experienced is caused by something else
- If the local router does not support IPSec Passthrough or NAT-Traversal, you probably need to change your VPN Tracker and/or gateway configuration

- If it supports neither IPSec Passthrough nor NAT-Traversal, you probably have to exchange the local router



Result

Local Router	192.168.40.1 00:06:B1:11:89:9C
IPSec Passthrough	✓
NAT-Traversal (old)	✓
NAT-Traversal (new)	✓

Summary: Your current Internet connection and local router fully support IPSec VPN with different NAT-Traversal versions. You should not experience any NAT-related problems when connecting to your VPN gateway.

Please refer to "IPSec Explained" for details on VPN traffic and NAT-Traversal.

Application Firewall

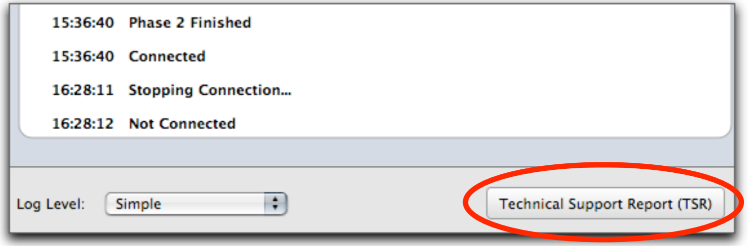
When using Mac OS X 10.5.1 or later with the application firewall enabled, you need to allow VPN Tracker to establish a connection explicitly. The option "Allow only essential services" will keep VPN Tracker from working properly.

Creating a Technical Support Report

If you cannot figure out how to solve the problem with the help of the log hints and/or the VPN Environment Manager, you should send a Technical Support Report (TSR) to equinux Support.

To create a Technical Support Report:

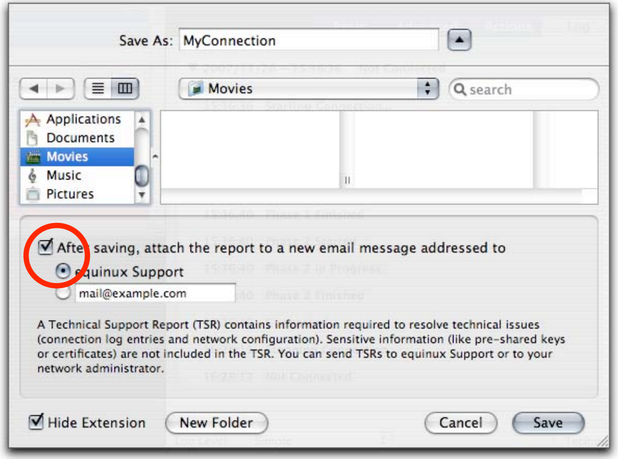
- Click the yellow triangle next to the connection slider
- Click the TSR button below the log



```
15:36:40   Phase 2 Finished
15:36:40   Connected
16:28:11   Stopping Connection…
16:28:12   Not Connected
```

Log Level: Simple

- Select the options as indicated on the screenshot below



Save As: MyConnection

☑ After saving, attach the report to a new email message addressed to

● equinux Support

○ mail@example.com

A Technical Support Report (TSR) contains information required to resolve technical issues (connection log entries and network configuration). Sensitive information (like pre-shared keys or certificates) are not included in the TSR. You can send TSRs to equinux Support or to your network administrator.

☑ Hide Extension

- Click "Save"
- Enter your local administrator password to save the TSR

If you're using Apple Mail as your default email client, a message to equinux Support will be opened automatically.

- Add your comments to the message template
- Send the message

For other email clients:

- Please create a message manually and attach the TSR
- Add comments to the message, if necessary
- Send the message

Missing Device Profiles

In many cases, the device profiles included in VPN Tracker will simplify setting up a device. However, the device profiles won't help in two cases:

- The VPN gateway has not been tested with VPN Tracker, so there is no device profile, and equinux cannot provide support
- The gateway's VPN settings have been modified, so the device profile in VPN Tracker does not match the actual settings

If you have administrative access to the gateway yourself, please refer to "Custom Devices" for instructions on creating new device profiles, or modifying existing ones.

If you don't have access to the device yourself, you will need to contact the network administrator, as described in the next section.

Assisted Troubleshooting

In an ideal world, your network administrator uses a Mac and provided a connection profile for you to import (or even a deployment bundle). But in this world, you wouldn't have to read this troubleshooting chapter.

If you have limited networking experience, and the VPN Tracker log does not help, the best solution for any configuration problem is to create a TSR, and send it to the network administrator so he/she can tell you how configure VPN Tracker.

Please read the following instructions carefully, so your admin gets all the information he/she needs to assist you.

Sending a TSR to a Mac-based Admin

To send a TSR to an administrator using a Mac, just follow the instructions at the beginning of this chapter, but enter your administrator's email address as the recipient.

TIP If your admin uses a Mac anyway, and there's more than one Mac user to support, we strongly recommend to get one VPN Tracker Professional license, so the admin can create and export connection profiles.

Sending a TSR to a Windows-based Admin

A TSR is a disk image file which can be opened on Macs only.

If your administrator has access to Windows PCs only:

- Do not send the TSR file directly
- Doubleclick the TSR file to open it
- Copy all files and folders into a separate folder
- Right-click that folder and select "Create archive of..."
- Send the zipped folder to your administrator manually

Appendix: Preferences

Most preferences in VPN Tracker are connection-specific and are touched in the section regarding custom connections. There's only a small set of truly global options.

Updates

VPN Tracker is updated regularly, and you can instruct the application to check for updates (and notify you).

To make VPN Tracker check for updates automatically:

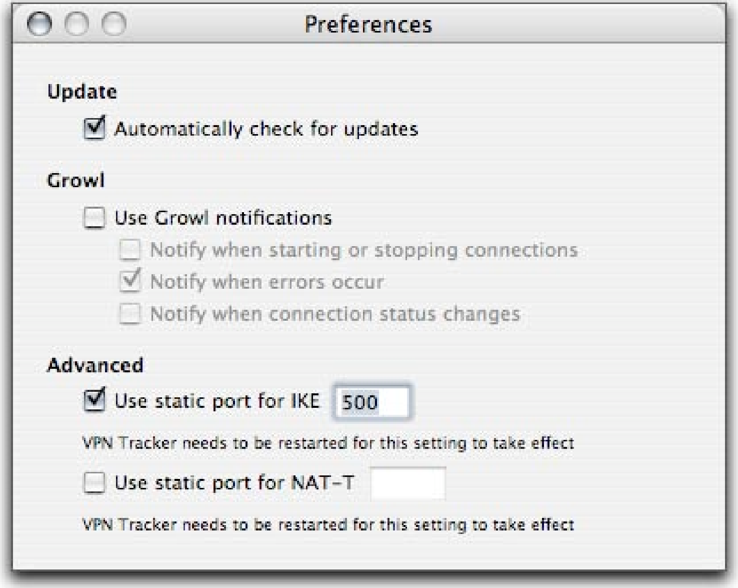
- Check the appropriate box in the preferences

Growl

Growl is a system-wide notification tool. VPN Tracker can display Growl notifications for starting or stopping connections, for errors or even when a connection status changes

To enable Growl:

- Check the appropriate box
- Activate the desired notifications



Preferences

Update

☑ Automatically check for updates

Growl

☐ Use Growl notifications

☐ Notify when starting or stopping connections

☑ Notify when errors occur

☐ Notify when connection status changes

Advanced

☑ Use static port for IKE 500

VPN Tracker needs to be restarted for this setting to take effect

☐ Use static port for NAT-T

VPN Tracker needs to be restarted for this setting to take effect

Advanced (Ports)

In certain network environments (e.g. when using the Back to my Mac feature in Mac OS X 10.5), dynamic port handling is required.

To enable dynamic ports for IKE or NAT-T:

- Uncheck the appropriate box

Appendix: IPSec Explained

IPSec – The Standard

Virtual Private Networks (VPN) are all about transmitting sensitive information over unprotected networks. This setup is often illustrated using a "tunnel" metaphor – protected data is sent through a secure VPN tunnel.

A VPN connection can, for example, link two local area networks (LANs) or a remote dialup user and a LAN. The traffic that flows between these two points passes through shared resources such as routers, switches and other network equipment that make up the public Internet.

A lot of information is exchanged using the IP protocol – the fundament of the Internet. Unfortunately, the IP protocol has no security mechanisms at all – confidentiality, integrity and authenticity of IP packets cannot be ensured by the protocol specification. This is where IPSec comes into play. IPSec builds on the IP specification to create secure "tunnels" within a public network (such as the Internet). Being fast and reliable, it quickly became the most established standard for VPN connections in IP networks. Many vendors (such as Cisco, SonicWALL, Watchguard, and others) offer gateways implementing IPSec for secure connections.

VPN Tracker also uses IPSec, and is inherently compatible with all devices providing a standard IPSec implementation. Unfortunately, some vendors decided to create "useful" undocumented proprietary extensions to the public standard. Not all of these extensions are implemented in VPN Tracker.

Using IPSec, VPN Tracker provides

- Privacy (via encryption)
- Content integrity (via data authentication)
- Sender authentication
- Non-repudiation (via data origin authentication, if using certificates)

Establishing a VPN Tunnel

An IPsec tunnel consists of a pair of unidirectional **Security Associations** (SAs) – one at each end of the tunnel – that specify the security parameters and the source and destination IP addresses. Since an SA defines a tunnel, the terms "SA" and "(VPN) tunnel" can be used interchangeably.

Before sending information through a VPN tunnel, the two partners need to obtain a secret key to encrypt and authenticate the data. While it is allowed by the IPSec specification to create such a key manually, it is both unflexible and potentially insecure.

In most environments, the automated **Internet Key Exchange (IKE)** standard is preferred. Strictly speaking, IKE is not part of the IPSec standard. It inherits from other standards (**ISAKMP, Oakley** and **SKEME**) and describes how to generate SAs for various purposes.

Phase 1 and Phase 2

Generating SAs according to IKE requires two phases. **Phase 1** is defined according to the ISAKMP standard, and generates an ISAKMP-SA (or IKE-SA). Two modes are defined: The faster **Aggressive Mode** uses three messages, while the more secure **Main Mode** uses six (three two-way exchanges). Because the participants' identities are not exchanged securely in Aggressive Mode, it does not provide identity protection.

The tunnel established in Phase 1 is used in **Phase 2** (Quick Mode) to generate an IPSec-SA. Simply put: Phase 1 authenticates the peers, while Phase 2 configures the actual VPN tunnel.

It may seem odd to use an SA (a Phase 1 tunnel) to create another SA (a Phase 2 tunnel), but there are a number of good reasons for this:

- A single ISAKMP-SA can be used to create multiple IPSec-SAs
- All authentication takes place in Phase 1, so the conversation in Phase 2 can be restricted to the actual IPSec parameters
- The separation of phases maintains the independence of IKE and IPSec – IKE is not restricted to creating IPSec-SAs in Phase 2, and IPSec-SAs can be created according to other standards

Proposals

In both phases, the participants need to agree upon at least one proposal, i.e. a combination of

- An encryption algorithm
- A hash algorithm (which is used for authentication in Phase 2)
- A Diffie-Hellman group (which is optional in Phase 2).

These parameters are used to generate SAs based on a pre-shared key or on certficates.

Authentication

To authenticate the peers in Phase 1, IKE uses either a **Pre-shared Key (PSK)**, or **Certificates**. A PSK is nothing but a password known to both peers. Digital certificates are generally regarded as the best solution for determining user identity with absolute confidentiality. A digital certificate is an electronic document used to identify a single user, a server or a company. Each certificate is signed by a trusted **Certificate Authority (CA)**.

The two standard authentication methods can be complemented by **Extended Authentication (XAUTH)**, an extension to IKE. XAUTH defines an additional user authentication in a separate phase right after Phase 1 (but before the beginning of Phase 2).

The user authentication can be checked against an internal database in the VPN device or external databases, e.g. against a

RADIUS or LDAP server. This allows the user to use the same login information for the VPN connection and other services (like email or file services).

The different authentication passwords tend to create some confusion. There are usually three passwords involved in using VPN Tracker:

- The password for the local user account on your Mac. If your account is an admin account, you can also use this password to install VPN Tracker. If not, you will need a local admin password for installing VPN Tracker
- The connection password (pre-shared key) which is usually unique for each connection, but shared by all users of a connection
- The XAUTH password and username are used to identify your VPN connection among all users connecting with the same pre-shared key

Encryption

An encryption algorithm is a method of converting a plaintext message into an alternate ciphertext message using a known key. The ciphertext message contains all the information of the plaintext message, but is not in a format readable by a human or computer. The ciphertext message can be decrypted to the original plaintext message using the same key used for encryption. For IPsec connections, both participants of the connection compute a secret key during connection establishment which is later used to encrypt and decrypt the packets.

There are several algorithms available for encryption purposes. The older ones (like **DES**) are considered to be breakable in principle, so it is recommended to use either **3DES** or **AES**.

AES (Advanced Encryption Standard) is a symmetric block cipher algorithm approved by the Federal Information Processing Standard (FIPS) for use by U.S. Government organizations (and others) to protect sensitive information. It was originally developed under the name "Rijndael" as a candidate algorithm for a worldwide competition to develop a new encryption technique that can be used to protect sensitive information in federal computer systems. The competition was organized by the U.S. National Institute of Standards and Technology (NIST) and the U.S. Commerce Department's Technology Administration. VPN Tracker implements the AES algorithm with key lengths of 128, 192 and 256 bits for encrypting ISAKMP and IPsec packets.

Tunnel Lifetimes

An interesting aspect of Phase 1 and Phase 2 tunnels are their respective lifetimes. Each SA has an explicit lifetime, after which it expires. This means that a long-lived Phase 1 tunnel can be used to establish multiple short-lived Phase 2 tunnels. The only requirement is that both peers use the same lifetime for a certain SA.

Since a Phase 1 tunnel is only used to negotiate a Phase 2 tunnel (i.e. there is very few data transferred through it), it is extremely hard to hack after it has been established. A Phase 2 tunnel, on the other hand, is protected by a Phase 1 tunnel while being established, so it's practically hackable only after it has been established.

So in theory, you should choose a longer lifetime for Phase 1 and a shorter lifetime for Phase 2 for optimal security. Practically, it is almost impossible to hack a 3DES tunnel (or even an AES tunnel), even with specialized equipment.

Transport vs. Tunnel Mode

IPsec operates in one of two modes: transport or tunnel. When both ends of the tunnel are hosts, you can use transport mode or tunnel mode. When at least one of the endpoints of a tunnel is a security gateway, such as a router or firewall, you must use tunnel mode. VPN Tracker can operate in tunnel and transport mode for IPsec tunnels.

In transport mode, the original IP packet is not encapsulated within another IP packet. The entire packet can be authenticated, the payload can be encrypted (with ESP), and the original header remains in plaintext as it is sent across the Internet.

In tunnel mode, the entire original IP packet – payload and header – is encapsulated within another IP payload and a new header appended to it. The entire original packet can be encrypted with ESP.

UDP and AH vs. ESP

While a tunnel is being established, the IKE communication between the peers consists of UDP packets sent to port 500.

Once a tunnel is established, IPsec uses one of two protocols to secure communications at the IP layer. **Authentication Header (AH)** is a security protocol for authenticating the source of an IP packet and verifying the integrity of its content. This protocol is not used by VPN Tracker, because ESP provides superior capabilities. **Encapsulating Security Payload (ESP)** is a security protocol for encrypting the entire IP packet (in addition to authenticating the source and ensuring the content integrity like AH).

ESP ensures the privacy, authenticity and integrity of all data sent through an IPSec tunnel.

NAT-Traversal

Network Address Translation (NAT)

If a connection has been configured correctly, almost all problems can be traced back to **Network Address Translation (NAT)** and its fundamental incompatibility with IPSec tunnels.

Most of today's internal networks are using private IP ranges (e.g. 192.168.36.0/24), with a NAT router acting as the default gateway. This router translates private IPs to a single public IP: The original source IP of outgoing packets is switched to the public IP of the router (so all response packets are sent to the router directly).

If there is more than a single host in the private network accessing the same host, the router obviously needs to distinguish the response packets somehow.

This is achieved by mapping the original client's source port (and its private IP address) to unique ports by the router. The router the relation between these addresses in a mapping table. When the response packet arrives at the router, it checks the table to find out where to send the data and translates the IP headers back to the originating private IP and source port.

NAT effectively prevents exposing the internal addresses and enables hosts with private IP addresses to communicate on the Internet.

NAT and ESP

How does this affect IPSec tunnels? Remember that IKE uses UDP packets to negotiate a tunnel, but ESP packets to transfer the actual data.

The ESP protocol has no ports (unlike UDP or TCP), so the NAT method cannot be used to translate ESP packets from private to public addresses and back.

IPSec Passthrough

The simplest solution to this dilemma is called IPSec Passthrough. Routers supporting this technique will just send ESP responses back to the last host who contacted the remote gateway. This obviously does not work if more than a single host needs to establish a VPN connection.

Traversing the Problem

NAT-Traversal is generally considered a reliable and more flexible solution: Before sending out an ESP packet, the VPN participant encapsulates it by adding an additional UDP header.

This UDP header can be altered by the NAT router. Since the additional header is removed by the remote peer **before** checking the ESP packet, changing it does not affect the integrity of the packets.

After removing the UDP header, the enclosed packet is analyzed. If it is considered to be authentic and unchanged, the remote peer will also use NAT-T to send its response.

The only issue with NAT-T is that different drafts of the NAT-T specification recommend different UDP ports to use. Initial drafts used port 500, which caused some devices (routers) between the VPN peers and VPN gateway to drop the packets (as they expected IKE/ISAKMP packets on that port only).

Newer drafts recommend "port-floating", i.e. a switch from UDP port 500 to port 4500 while the tunnel is being established. If the remote VPN gateway supports port floating, this should work fine (unless the administrator of an intermediate firewall did not open that port).

Client Provisioning and Mode Config

Client Provisioning provides a means to receive configuration parameters from the VPN gateway. This needs to be supported by the VPN gateway and enabled for the connection.

There are many different vendor-specific implementations of Client Provisioning. VPN Tracker supports Client Provisioning for SonicWALL (DHCP over IPSec) and Cisco.

Mode Config is a similar, but vendor-independent mechanism to Client Provisioning, which usually supports fewer configuration parameters. VPN Tracker supports Mode Config connections to Cisco (Cisco's client provisioning is an extension to Mode Config) and Juniper Netscreen devices.

Note Other vendors using the same implementation of Mode Config might also be supported, but this has not been tested yet.

Gateways may provide one or more of the following paramters using Client Provisioning or Mode Config:

- Local Address (virtual IP)
- DNS Settings
- Remote Networks