equinux

VPN Tracker 365

VPN Configuration Guide

Securepoint

NextGen UTM Firewalls

Revised May 2021

www.equinux.com

Contents

Introduction

My VPN Gateway Configuration Checklist

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

Pre-Shared Key

(1) Pre-Shared Key: _____

IP Addresses

(1) WAN IP Address: _____._____._____._____ (or hostname _____)

(2) LAN (internal) IP Address / Subnet Mask: _____._____._____._____ / _____._____._____.

User Authentication (XAUTH)

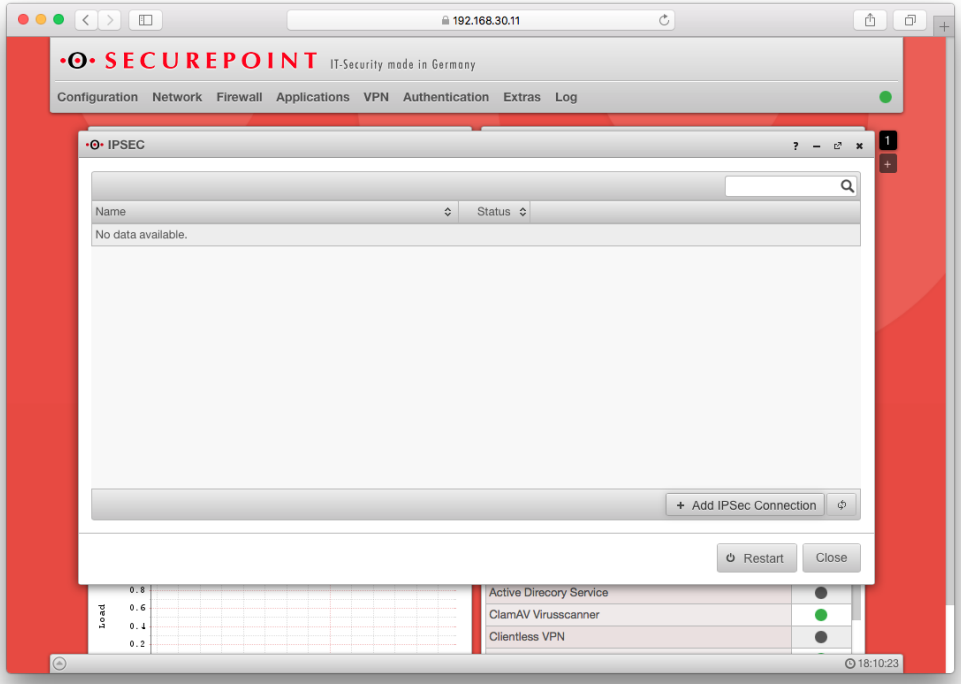
(4) Username: _____

(5) Password: _____

Task 1 – VPN Gateway Configuration

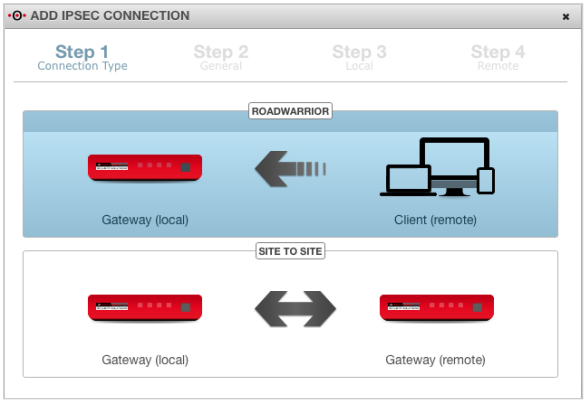
Step 1 – Add an IPSec connection on the device

- ➔ Connect to your VPN gateway through its web interface
- ➔ Go to the VPN > IPSec tab
- ➔ Select + Add IPSec Connection

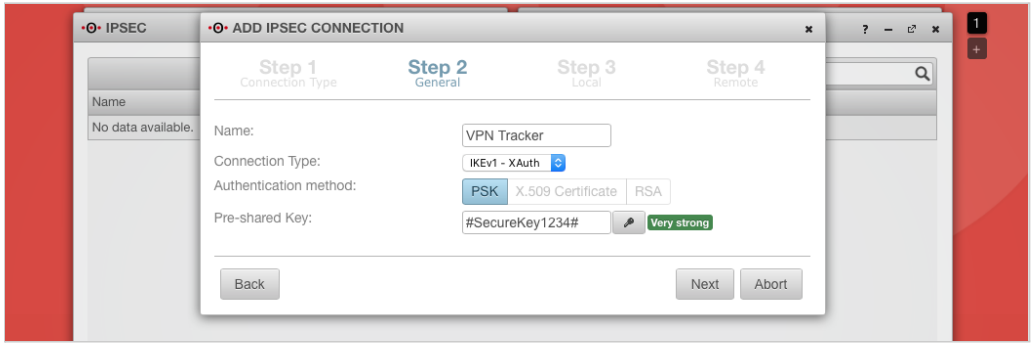


Step 2 – Configure the IPSec connection

➔ Connection Type: choose **Roadwarrior**



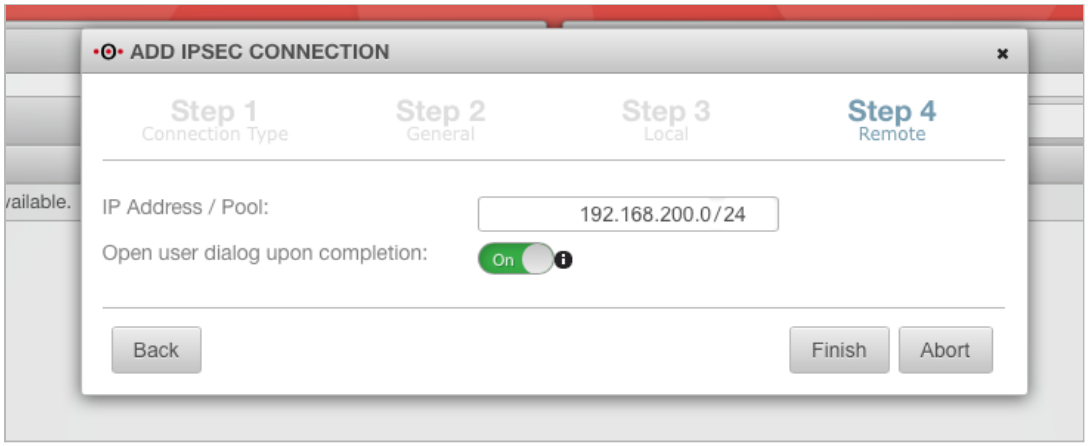
➔ Next, enter a name for your connection and select **IKEv1** as the connection type and **PSK** as the authentication method.
➔ Generate your pre-shared key and write this down as **(1)** on your configuration checklist, then click **Next** to proceed.



➔ Choose **Any Interface** and carry on to the next step.

➔ Enter a new **IP Address Pool** that will be used to assign VPN users an IP address. Be sure to choose a network that is distinct from the networks you want to access over VPN.

➔ Write this down as **(3)** on your configuration checklist, then click **Finish**.



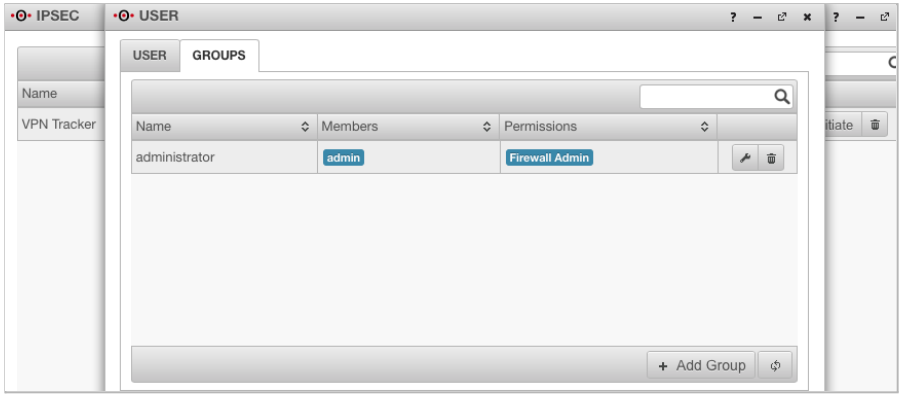
Step 3 – Add Users and assign them to Groups

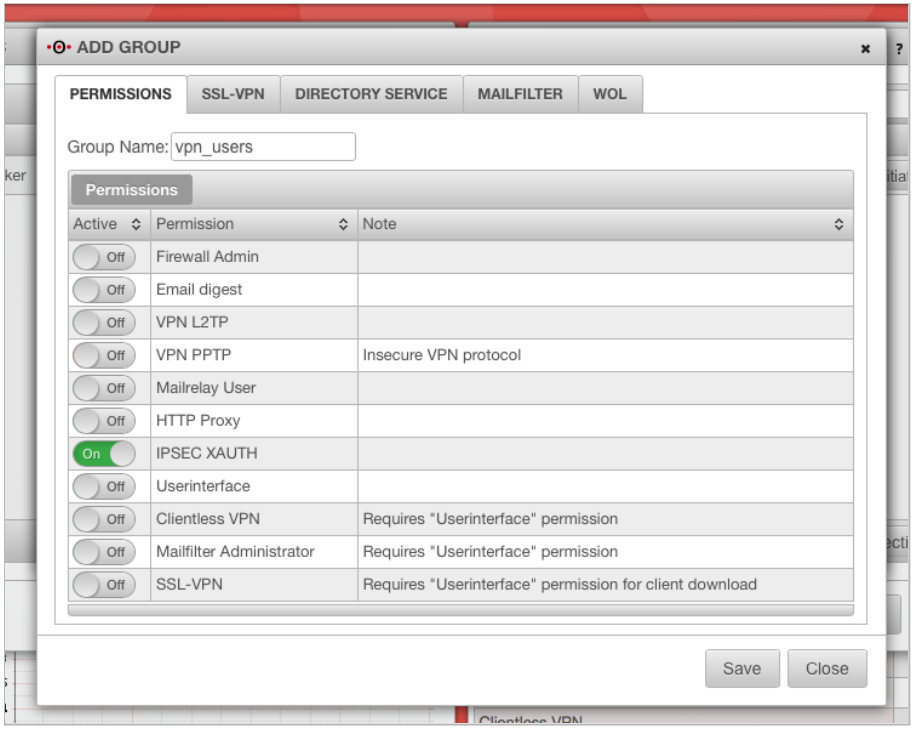
After you click Finish, a **User** configuration window will automatically open. You can access these settings manually at any time via **Authentication > User.**

Set up a new group

➔ Switch to the **Groups** tab and click **Add Group.**

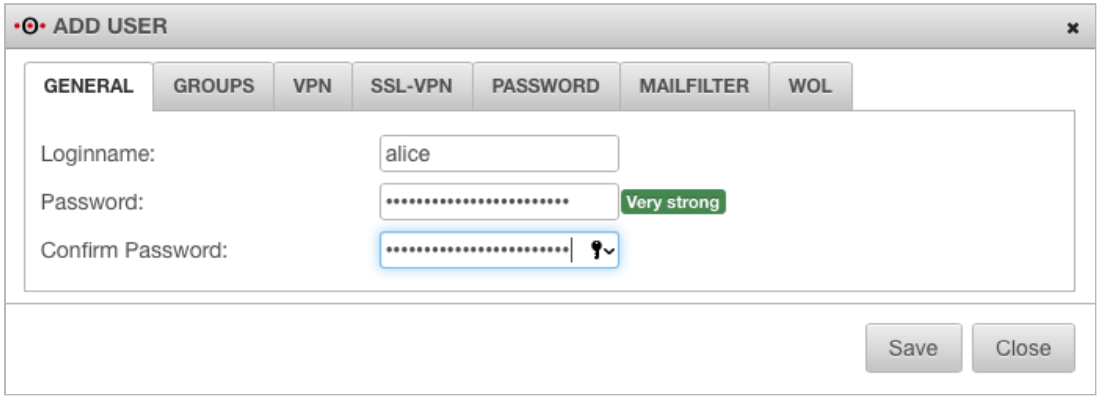
➔ In the **Permissions** tab, enter a **Group Name** and click the slider to activate **IPSEC XAUTH** for this group. Then click **Save**.





Add a new user

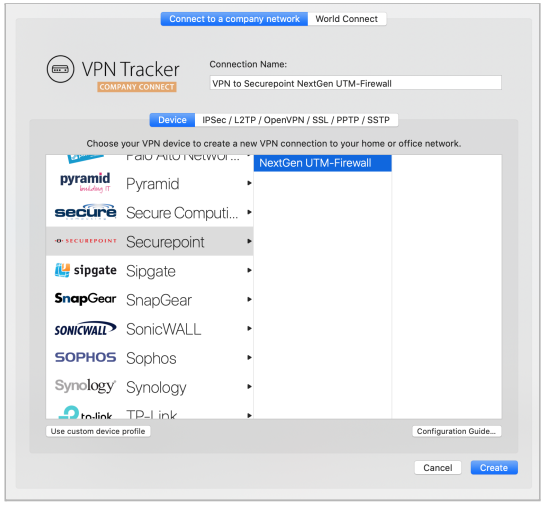
- ➔ Switch to the **User** tab and click **Add User**.
- ➔ On the **General** tab, create a **Loginname** and **Password** for the new user. Write these down as **(4)** and **(5)** on your checklist.
- ➔ On the **Groups** tab, select the user group you just set up to add the new user to it.



Click **Close** and on the **IPSec** tab, click **Restart** to end the configuration process. If you need to, you can always add more users by repeating the previous steps.

Task 2 – VPN Tracker Configuration

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



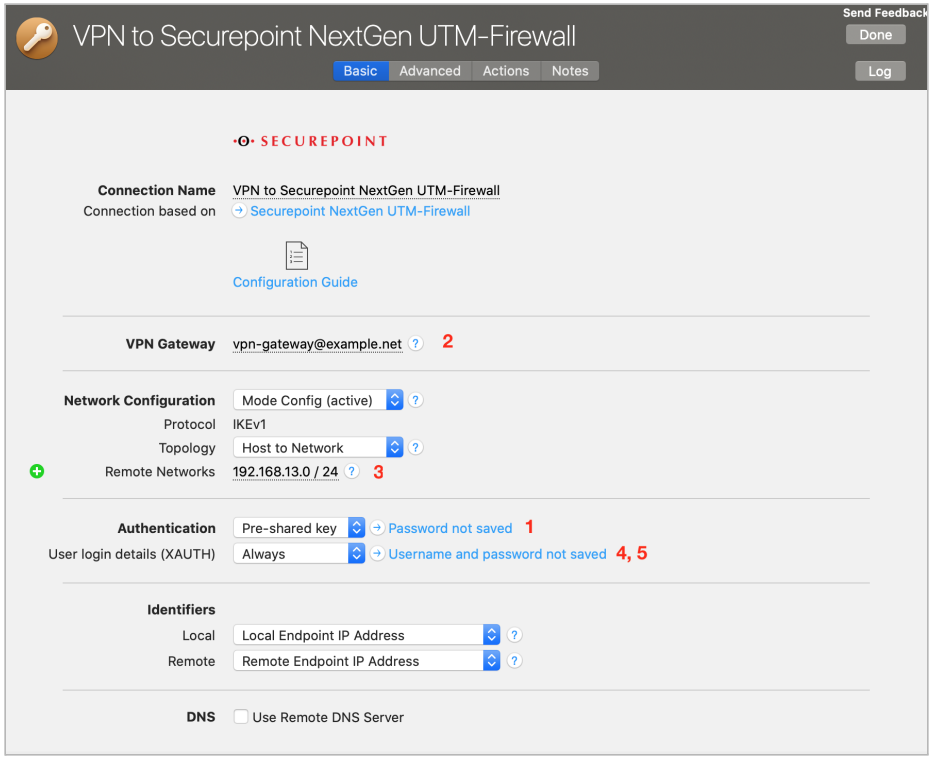
Step 1: Add a connection

- ➔ Open VPN Tracker 365.
- ➔ Click on the + in the bottom left corner of the app window and select "**Create new Company Connection**"
- ➔ Select **Securepoint** from the list.
- ➔ Select your model (e.g. NextGen UTM Firewall) and enter a name for your connection.

Step 2 – Configure the VPN Connection

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

- ➔ **VPN Gateway**: Enter the WAN IP address (or hostname) of your VPN gateway that you wrote down as **(2)**
- ➔ **Remote Networks**: Enter the network address of the network that is being accessed through the VPN tunnel **(3)**. Separate the subnet mask with a forward slash („/")
- ➔ Under **Authentication**, enter the **Pre-Shared Key (1)** you configured earlier on. 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.
- ➔ Then, by **XAUTH**, enter your user credentials **(4)** and **(5)**
- ➔ Click **Done** to save your settings.



Task 3 - Testing the VPN connection

In order to test your connection, you will need to connect from a different location.

For example, if you are setting up a VPN connection to your office, try it out at home, or from an Internet cafe, or go visit a friend.

Connect to your VPN

- ➔ Check first of all that your internet connection is working as it should be. Use this link as a test: http://www.equinux.com
- ➔ Start the VPN Tracker 365 app.
- ➔ Click on the On/Off slider to turn on your connection.

IMPORTANT:

If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection. Wait for the test to complete.

Connected!

Connecting may take a couple of seconds. If the On/Off button turns blue that's great – you're connected! Now is a great time to take a look at the VPN Tracker Manual. It shows you how to use your VPN and how to get the most out of it.

Troubleshooting

In case there's a problem connecting, a yellow warning triangle will show up. Click the yellow warning triangle to be taken to the log.

The log will explain exactly what the problem is. Follow the steps listed in the log.

TIP: Press Cmd-L to open the log in a new window. That way, you can have the log side-by-side with your VPN configuration while making changes to troubleshoot a problem.

VPN Tracker Manual

The VPN Tracker Manual contains detailed troubleshooting advice. Answers to frequently asked questions (FAQs) can be found at: http://www.vpntracker.com/support

Technical Support

If you're stuck, the technical support team at equinux is here to help. Contact us via http://www.vpntracker.com/support

Please include the following information with any request for support:

- ➔ A description of the problem and any troubleshooting steps that you have already taken.
- ➔ A VPN Tracker Technical Support Report (Log > Technical Support Report).
- ➔ Device model and the firmware version running on it.
- ➔ Screenshots of the VPN settings on your VPN gateway.

IMPORTANT: A Technical Support Report contains the settings and logs necessary for resolving technical problems. Confidential information (e.g. passwords, private keys for certificates) is not included in a Technical Support Report.