



# VPN Tracker 365

## VPN Configuration Guide

Zyxel

USG Series, USG Flex Series, ZyWALL VPN Firewalls, ZyWALL ATP Firewalls

© 2020 equinix AG and equinix USA, Inc. All rights reserved.

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

The equinix logo is a trademark of equinix AG and equinix USA, Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

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

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

Revised November 2020

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

[www.equinix.com](http://www.equinix.com)

# Contents

## **Introduction**

[My VPN Gateway Configuration Checklist](#)

## **Task 1 – VPN Gateway Configuration**

## **Task 2 – VPN Tracker Configuration**

[Step 1 – Add a Connection](#)

[Step 2 – Configure the VPN Connection](#)

## **Task Three - Testing the VPN connection**

[Connect to your VPN](#)

[Troubleshooting](#)

[Technical Support](#)

# 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 ZyWALL USG VPN gateway device.

### IP Addresses

(1) WAN IP Address: \_\_\_\_\_ (or hostname \_\_\_\_\_)

(2) LAN (internal) IP Address / Subnet Mask: \_\_\_\_\_ / \_\_\_\_\_

### User Authentication (XAUTH)

(3) Username: \_\_\_\_\_

(4) Password: \_\_\_\_\_

### Pre-Shared Key

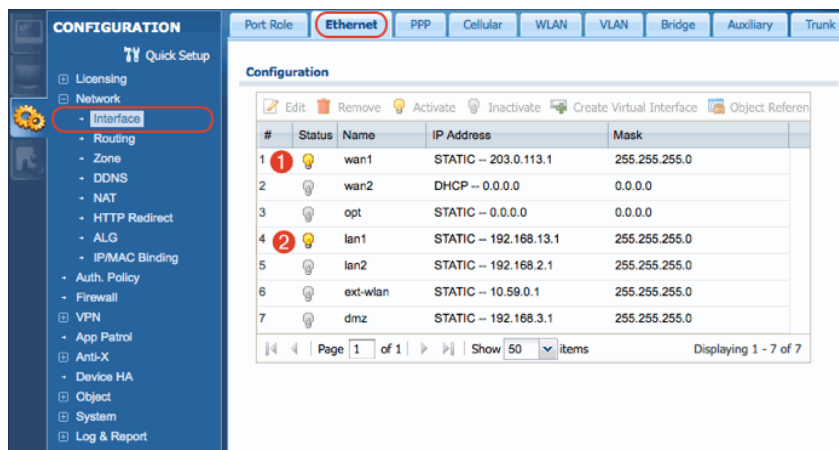
(5) Pre-Shared Key: \_\_\_\_\_

# Task 1 – VPN Gateway Configuration

We will first set up VPN on the VPN gateway. If you already have VPN in place, it's helpful to follow this tutorial to see how settings on the device fit together with VPN Tracker.

## Step 1 – Retrieve Network Settings

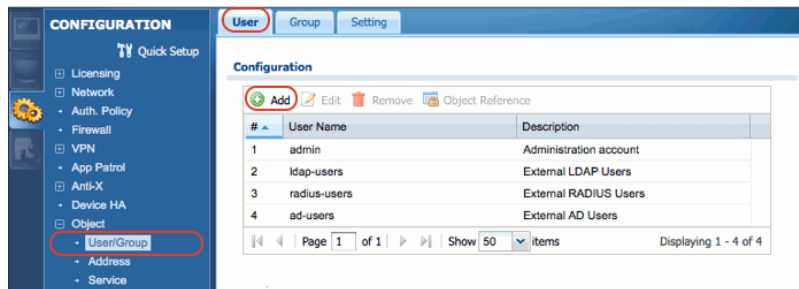
- Connect to your VPN gateway through its web configuration interface
- Go to the **CONFIGURATION** tab to access the device's settings
- Go to **Network > Interface** and switch to the **Ethernet** tab:



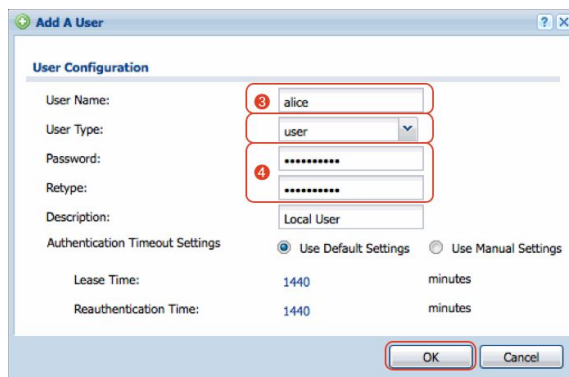
- Write down the IP address of the primary **WAN** network interface (here: **wan1**) as **(1)** on your *Configuration Checklist*. If your device has a DNS hostname (fixed or DynDNS), write it down instead
- Write down the IP address of the **LAN** network interface (here: **lan1**), including its **subnet mask** as **(2)** on your *Configuration Checklist*

## Step 2 – Create a VPN User

→ Go to **Object > User/Group** and switch to the **User** tab. Then, click the **Add** button:



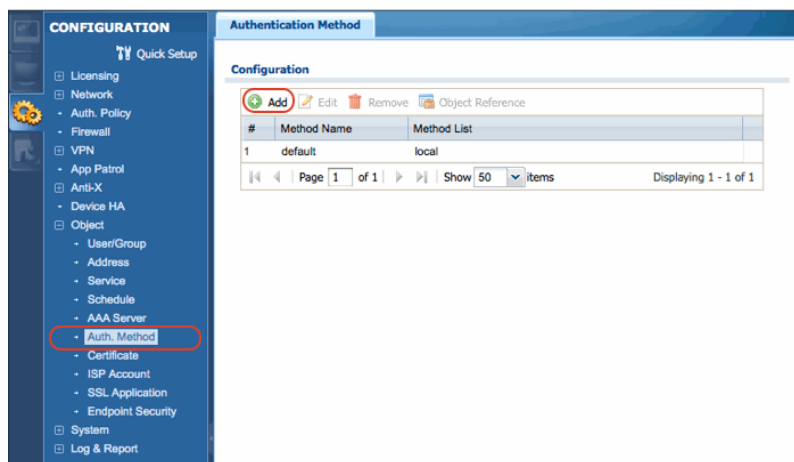
- **User Name:** Enter a username for the new user (here: **alice**). Write down the user name as **(3)**
- **User Type:** Choose **user** from the pop-up
- **Password:** Enter a password for this new user. Make sure to remember the password, or write it down as **(4)** then click **OK** to add the user



To add more users, simply repeat this step. You might want to connect the device to an existing (LDAP or RADIUS) authentication server later (remember to select the appropriate user type for the external authentication server in the **User Type** pop-up). We recommend using a local user for initial setup and testing.

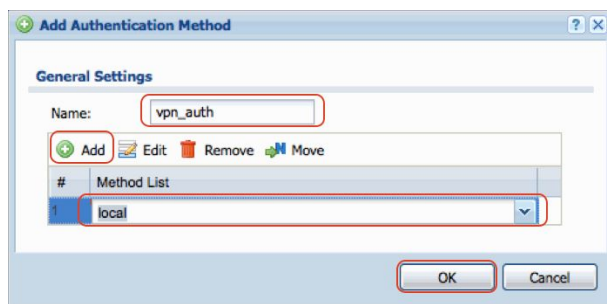
## Step 3 – Create an Authentication Method

→ Go to **Object > Auth. Method** and click the **Add** button:



→ **Name:** Enter a name for the new authentication method (here: **vpn\_auth**)

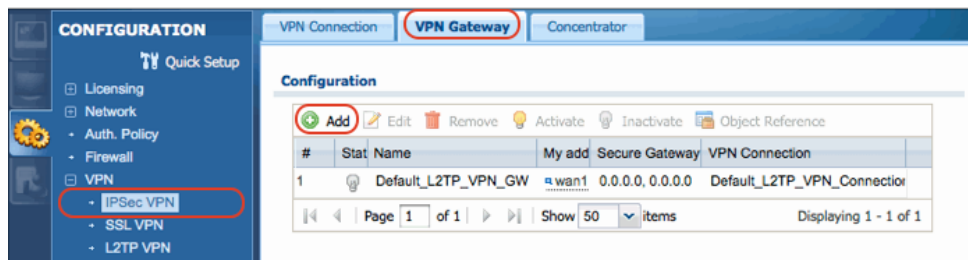
→ Click the **Add** button and choose **local** from the pop-up



→ Click **OK** to save the authentication method

## Step 4 – Set up Phase 1

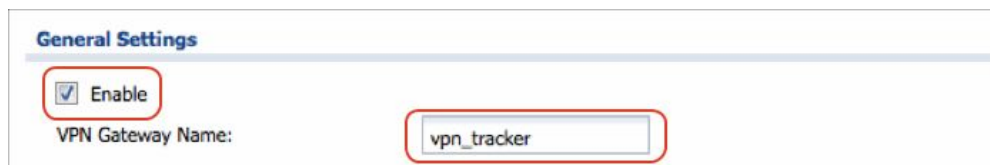
→ Go to **VPN > IPsec VPN** and switch to the **VPN Gateway** tab. Click the **Add** button:



→ Click the **Show Advanced Settings** button to be able to access all settings



### General Settings



- Select the **Enable** checkbox to enable the VPN gateway settings that you are about to configure
- **VPN Gateway Name:** Enter a name for the phase 1 setup (here: **vpn\_tracker**)



## Gateway Settings

**Gateway Settings**

**My Address**

☒ Interface wan1 Static -- 203.0.113.1/  
255.255.255.0

☐ Domain Name / IP

**Peer Gateway Address**

☐ Static Address

Primary 0.0.0.0

Secondary 0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

☒ Dynamic Address

- **My Address:** Select **Interface** and select your primary **WAN** network interface (here: **wan1**) from the pop-up menu
- **Peer Gateway Address:** Select **Dynamic Address**

## Authentication

**Authentication**

☒ Pre-Shared Key 5 topsecret

☐ Certificate

Local ID Type: IP


Content: 0.0.0.0

Peer ID Type: Any

Content:

- Enter a **Pre-Shared Key** (here: **topsecret**). Make sure to choose a good pre-shared key and remember it, or write it down as **(5)**
- **Local ID Type:** Make sure **IP** is selected
- **Content:** Leave the default of **0.0.0.0**. This means that the IP address entered for **My Address** will automatically be used as the device's identifier
- **Peer ID Type:** Make sure **Any** is selected. This means that connecting VPN clients can use any identifier type

## Phase 1 Settings



**Phase 1 Settings**

SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Proposal

#	Encryption	Authentication
1	3DES	SHA1
2	AES128	SHA1

Key Group: DH2

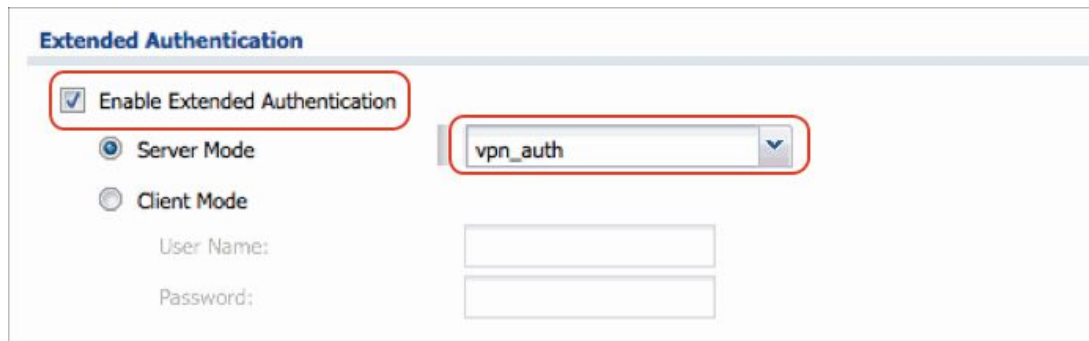
☒ NAT Traversal

☒ Dead Peer Detection (DPD)

- **SA Life Time:** Leave the default of 86400 seconds
- **Negotiation Mode:** Leave the default of **Main Mode**
- **Proposal:** For security reasons, we recommend changing the default proposal settings to use at least **3DES** and **SHA-1** (with the option of using **AES-128** and **SHA-1**) as shown here
- **Key Group:** Choose **DH2** from the pop-up
- Select the **NAT Traversal** checkbox
- Make sure the **Dead Peer Detection (DPD)** checkbox is selected

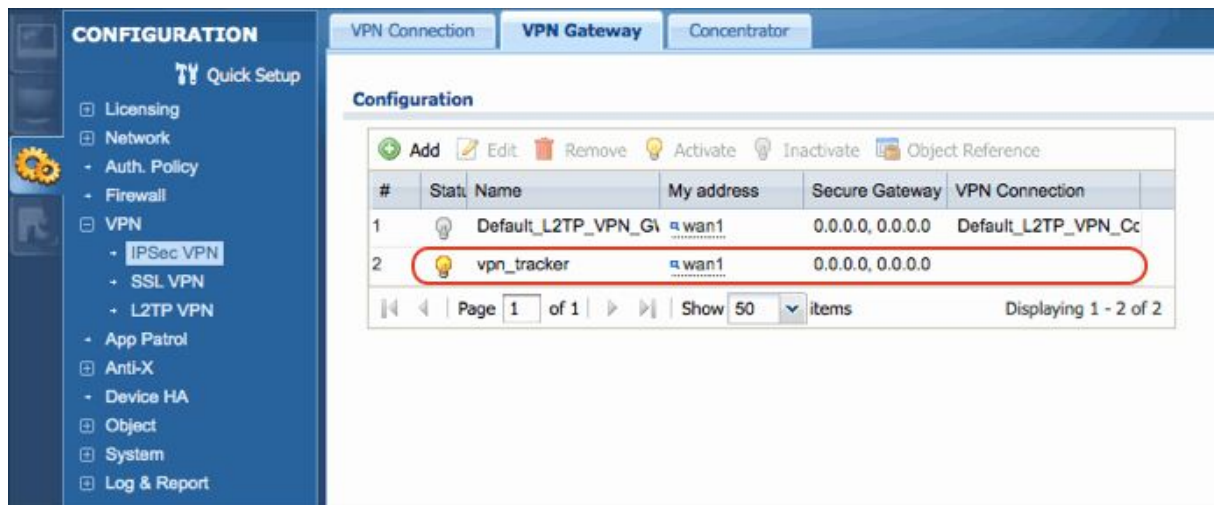
It is possible to use different phase 1 settings. Please note that any changes you make here must be matched in VPN Tracker (Advanced > Phase 1). We recommend using the settings shown here for initial setup and testing.

## Extended Authentication



The screenshot shows the 'Extended Authentication' configuration window. A red box highlights the 'Enable Extended Authentication' checkbox, which is checked. Below it, the 'Server Mode' radio button is selected. To the right of the radio buttons is a dropdown menu with 'vpn\_auth' selected. Below these are two empty text input fields labeled 'User Name:' and 'Password:'.

- Select the **Enable Extended Authentication** checkbox
- **Server Mode**: Choose **vpn\_auth** from the pop-up. If you do not see the vpn\_auth entry here, you may have skipped *Step 3 – Create an Authentication Method*
- Click **OK** to complete the phase 1 setup. The result should look similar to what is shown in the following screenshot:

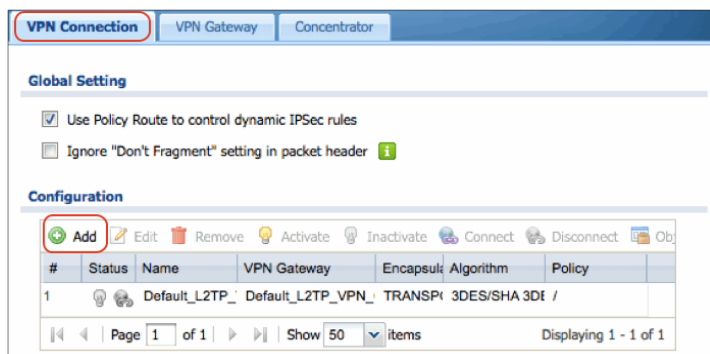


The screenshot shows the 'VPN Gateway' configuration window. The left sidebar has a tree view with 'VPN' expanded, showing 'IPSec VPN', 'SSL VPN', and 'L2TP VPN'. The main area has tabs for 'VPN Connection', 'VPN Gateway', and 'Concentrator'. The 'VPN Gateway' tab is active, showing a 'Configuration' table. The table has columns: '#', 'Status', 'Name', 'My address', 'Secure Gateway', and 'VPN Connection'. There are two entries: 1. 'Default\_L2TP\_VPN\_GW' with status 'Inactive' and 'wan1' address. 2. 'vpn\_tracker' with status 'Active' and 'wan1' address. A red box highlights the 'vpn\_tracker' row. Below the table is a pagination bar showing 'Page 1 of 1', 'Show 50 items', and 'Displaying 1 - 2 of 2'.

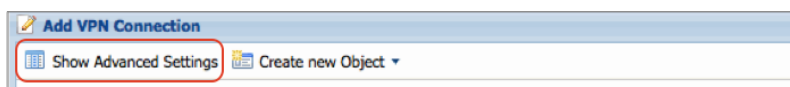
#	Status	Name	My address	Secure Gateway	VPN Connection
1	Inactive	Default_L2TP_VPN_GW	wan1	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Cc
2	Active	vpn_tracker	wan1	0.0.0.0, 0.0.0.0	

## Step 5 – Set up Phase 2

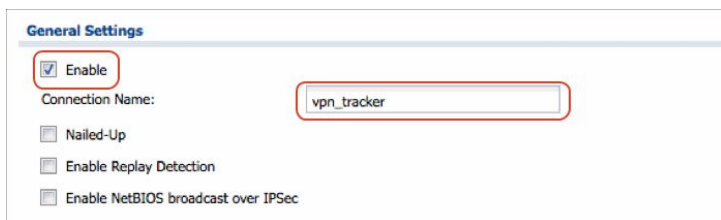
→ Switch to the **VPN Connection** tab (under **VPN > IPsec VPN**) and click the **Add** button:



→ Click the **Show Advanced Settings** button to be able to access all settings



### General Settings



- Select the **Enable** checkbox to enable the VPN connection settings that you are about to configure
- **Connection Name:** Enter a name for the phase 2 setup (here: **vpn\_tracker**)

## VPN Gateway

**VPN Gateway**

Application Scenario

☐ Site-to-site

☐ Site-to-site with Dynamic Peer

☒ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway: vpn\_tracker wan1 0.0.0.0 0.0.0.0

Manual Key

☐ Manual Key

- **Application Scenario:** Select **Remote Access (Server Role)**
- **VPN Gateway:** Choose the phase 1 (VPN gateway) setup you created in *Step 4* (here: **vpn\_tracker**) from the pop-up

## Policy

**Policy**

Local policy: LAN1\_SUBNET INTERFACE SUBNET, 192.168.13.0/24

☒ Policy Enforcement

- **Local policy:** Choose the address object corresponding to the network(s) VPN clients are permitted to access. Here, **LAN1\_SUBNET**, i.e. the ZyWALL's LAN network (2), is being used. This selection will be appropriate in most cases.
- Select the checkbox **Policy Enforcement** to restrict VPN client access to the network(s) chosen under **Local Policy**

## Phase 2 Settings

**Phase 2 Settings**

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

+ Add Edit Remove

#	Encryption	Authentication
1	3DES	SHA1
2	AES128	SHA1

Perfect Forward Secrecy (PFS): DH2

- **SA Life Time:** Leave the default of 86400 seconds
- **Active Protocol:** Leave the default of **ESP**
- **Encapsulation:** Leave the default of **Tunnel**
- **Proposal:** For security reasons, we recommend changing the default proposal settings to use at least **3DES** and **SHA-1** (with the option of using **AES-128** and **SHA-1**) as shown here
- **Perfect Forward Secrecy (PFS):** Choose **DH2** from the pop-up

It is possible to use different phase 2 settings. Please note that any changes you make here must be matched in VPN Tracker (Advanced > Phase 2). We recommend using the settings shown here for initial setup and testing.

## Related Settings

**Related Settings**

☒ Add this VPN connection to IPSec\_VPN zone.

- Make sure **Add this VPN connection to IPSec\_VPN zone** is selected. This means that any security rules or settings configured for the IPSec\_VPN zone will apply to this VPN connection. **Some devices may not have this option**, in that case, please add the connection manually to **Network > Zone**
- It is not necessary to make any changes to the **Connectivity Check** and **Inbound/Outbound traffic NAT** settings
- Click **OK** to complete the phase 2 setup. The result should look similar to what is shown in the following screenshot:

**CONFIGURATION**

Quick Setup

- Licensing
- Network
  - Auth. Policy
  - Firewall
- VPN
  - IPSec VPN**
  - SSL VPN
  - L2TP VPN
- App Patrol
- Anti-X
- Device HA
- Object
- System
- Log & Report

**VPN Connection** | VPN Gateway | Concentrator

**Global Setting**

- ☒ Use Policy Route to control dynamic IPSec rules
- ☐ Ignore "Don't Fragment" setting in packet header

**Configuration**

#	Status	Name	VPN Gateway	Encapsula	Algorithm	Policy
1		Default_L2TI	Default_L2TI	TRANSPC	3DES/SHA 3DES/MI	/
2		vpn_tracker	vpn_tracker	TUNNEL	3DES/SHA AES128	LAN1_SUBNET/0.0.

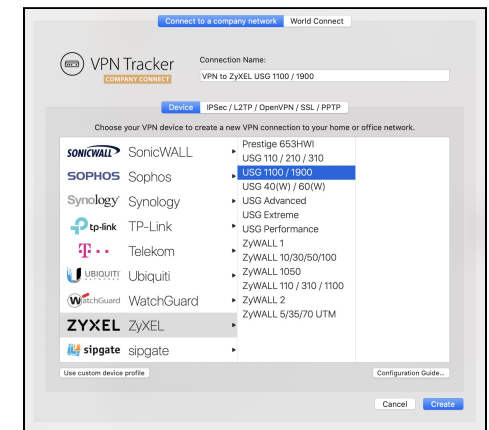
Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

## Task 2 – VPN Tracker Configuration

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

### Step One: 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 **Zyxel** from the list.
- Select your model (e.g. USG 1100/1900) and enter a name for your connection.

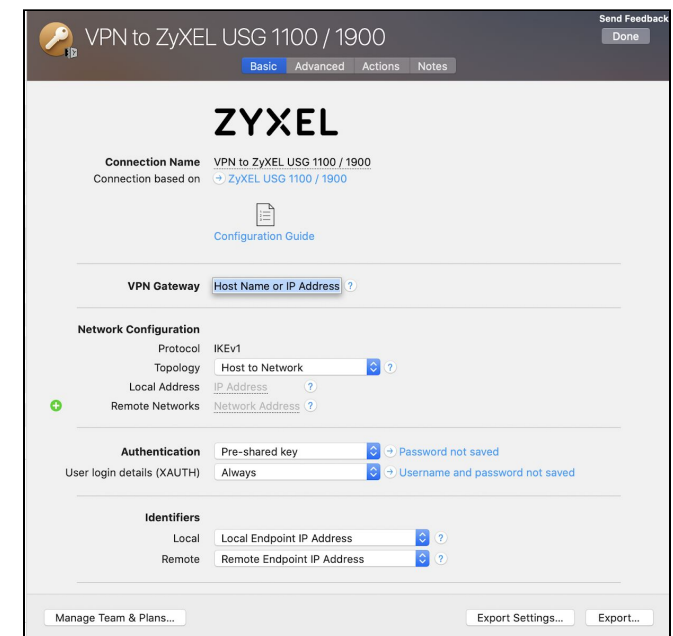


### Step 2 – Configure the VPN Connection

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 **(1)**
- **Local Address:** Leave empty for now. Depending on your setup, you may have to set a specific local address later. Refer to → *Supporting Multiple Users* on when and how to set a specific local address
- **Remote Networks:** Enter the network address of the network that is being accessed through the VPN tunnel **(2)**. Separate the subnet mask with a forward slash („/“)

**Tip:** VPN Tracker will automatically turn the IP address into a network address. Double-check that the result is the same as the LAN address object configured for the Local Policy in *Step 5*





## Task Three - 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.

- Depending on your setup, You will be prompted to enter your XAUTH username **(3)** and password **(4)** and your pre-shared key **(5)**. To save time for the future, 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.

### Connected!

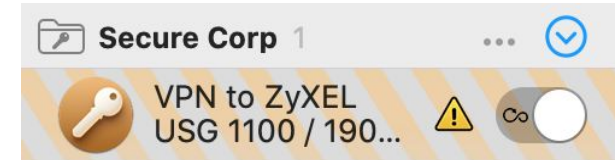
Connecting may take a couple of seconds. If the On/Off button turns blue that's great – you're connected! Now is a great time to take a look at the [VPN Tracker Manual](#). It shows you how to use your VPN and how to get the most out of it.

## 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](http://www.vpntracker.com/support) 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 equinix 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.