



VPN Tracker 365

VPN Configuration Guide

D-Link

DSR Series VPN Routers, DFL NetDefend UTM Firewalls

© 2021 equinux AG and equinux 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 equinux AG or equinux USA, Inc. Your rights to the software are governed by the accompanying software license agreement.

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

equinux 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 equinux 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. equinux is not responsible for printing or clerical errors.

Revised May 2021

Apple, the Apple logo, Mac, and macOS are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

Please note this guide is intended as a supplement to the documentation provided by your device's manufacturer and is not a replacement for the user manual.

www.equinux.com

Contents

Introduction

[My VPN Gateway Configuration Checklist](#)

Task 1 – VPN Gateway Configuration

[Step 1 – Address Book Entries](#)

[Step 2 – Create a Mode Config Pool](#)

[Step 3 – Add a Pre-Shared Key](#)

[Step 4 – Add an IPsec Interface](#)

[Step 5 – Add an XAUTH User](#)

[Step 6 – Add a User Authentication Rule](#)

[Step 7 – Add an Access Rule](#)

Task 2 – VPN Tracker Configuration

[Step 1: Add a connection](#)

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

Task 3 - Testing the VPN connection

[Troubleshooting](#)

[VPN Tracker Manual](#)

[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 device.

IP Addresses

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

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

Pre-Shared Key

(3) Pre-Shared Key: _____

User Authentication (XAUTH)

(4) Username: _____

(5) Password: _____

Task 1 – VPN Gateway Configuration

We will first set up VPN on the D-Link. If you already have a VPN set up, it's helpful to follow along this tutorial to see how settings on the D-Link fit together with VPN Tracker.

Step 1 – Address Book Entries

- Go to Objects > Address Book > Interface Addresses
- Find the wan1_ip entry in the list and write it down as **(1)** on your checklist
- Find the lan1net entry in the list and write it down as **(2)**

Mode Config Entries

VPN clients will be using Mode Config to automatically receive an IP address to use when connected through VPN. In our setup, we'll be using a pool of addresses that is independent from the D-Link's networks for VPN clients.

- Go to Objects > Address Book
- Click Add > IP Address
- **Name:** Enter a name that allows you to recognize the entry later (e.g. ModeConfigAddresses)
- **IP Address:** Enter the range of IP addresses that should be assigned to your VPN clients. The IP addresses should come from a private subnet that is not part of your D-Link's networks. In our example, we're using 10.13.95.100 - 10.13.95.199
- Click OK to save the entry

IP address
Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General User Authentication

General

Name: ModeConfigAddresses

IP Address: 10.13.95.100 - 10.13.95.199 e.g. "172.16.50.8", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"

Comments

Comments:

OK Cancel

For the Mode Config pool, we also need to specify the subnet mask of the network we've chosen:

- Click Add > IP Address
- **Name:** Enter a name that allows you to recognize the entry later (e.g. ModeConfigSubnet)
- **IP Address:** Enter the subnet mask of the network you have chosen for the address pool (e.g. 255.255.255.0)
- Click Ok to save the entry

IP address
Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General User Authentication

General

Name: ModeConfigSubnet

IP Address: 255.255.255.0 e.g. "172.16.50.8", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"

Comments

Comments:

OK Cancel

Step 2 – Create a Mode Config Pool

- Go to Objects > VPN Objects > Config Mode Pool
- Click Add > ConfigModePool
- Check the box **Use a Static IP Pool**
- **IP Pool:** Select the address book entry created in step 1
- **Netmask:** Select the address book entry for the subnet created in step 1
- Click OK to save the Mode Config pool

The screenshot shows the 'ConfigModePool' configuration window. The title bar reads 'ConfigModePool' with a subtitle: 'An IKE Config Mode Pool will dynamically assign the IP address, DNS server, WINS server etc. to the VPN client connecting to this gateway.' The window is divided into three main sections: 'General', 'Optional', and 'Comments'. In the 'General' section, the 'Use a Static IP Pool' radio button is selected. Below it, the 'IP Pool' dropdown is set to '(None)' and the 'Netmask' dropdown is set to 'ModeConfigSubnet'. The 'Optional' section contains four dropdown menus: 'DNS' (None), 'NBNS/WINS' (None), 'DHCP' (None), and 'Subnets' (None). The 'Comments' section has a text area for entering comments. At the bottom right, there are 'OK' and 'Cancel' buttons.

Tip: Mode Config pools can also use a reserved pool of addresses from a DHCP server. However, this limits the available VPN client addresses to the number of leases available on the DHCP server, and is more complex. We recommend going with a separate Mode Config pool first. You can always change to a DHCP server based address pool once you have everything working.

Step 3 – Add a Pre-Shared Key

- Go to Objects > Authentication Objects
- Click Add > Pre-Shared Key
- **Name:** Enter a name for the pre-shared key object (e.g. VPNTrackerPSK)
- Select **Passphrase**
- **Shared Secret:** Enter a password key for the connection and note this down on your checklist as **(3)**
- Click OK

The screenshot shows a 'Pre-shared key' configuration window. The title bar says 'Pre-shared key' with a key icon. Below the title bar, a subtitle reads: 'PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.' The window is divided into three sections: 'General', 'Shared Secret', and 'Comments'. In the 'General' section, the 'Name' field is filled with 'VPNTrackerPSK'. The 'Shared Secret' section has two radio buttons: 'Passphrase' (selected) and 'Hexadecimal Key'. Under 'Passphrase', there are 'Shared Secret' and 'Confirm Secret' fields, both containing asterisks. A red circle with the number '3' is next to the 'Shared Secret' field. Below these is a 'Passphrase' field and a 'Generate Random Key' button. A note at the bottom of the 'Shared Secret' section states: 'Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.' The 'Comments' section at the bottom has a 'Comments:' label and an empty text area. At the very bottom right are 'OK' and 'Cancel' buttons.

Step 4 – Add an IPsec Interface

- Go to Interfaces > IPsec
- Click Add > IPsec Tunnel

General

- Name: Enter a name for your tunnel (e.g. VPNTracker)
- Local Network: Select lan1net
- Remote Network: Select all-nets
- Remote Endpoint: Select all-nets
- Encapsulation Mode: Select Tunnel
- IKE Config Mode: Select Static (ConfigModePool)
- IKE Algorithms: Select High
- IKE Life Time: We'll be using the default lifetime of 28800 sec. If you ever decide to change this, you'll also need to modify the phase 1 lifetime in VPN Tracker
- IPsec Algorithms: Select High
- IPsec Life Time (seconds): We'll be using the default lifetime of 3600 sec. If you ever decide to change this, you'll also need to modify the phase 2 lifetime in VPN Tracker
- IPsec Life Time (kilobytes): The lifetime in kilobytes must be set to 0

The screenshot shows the configuration window for an IPsec tunnel. The 'General' tab is active, displaying fields for Name (VPNTracker), Local Network (lan1net), Remote Network (all-nets), Remote Endpoint (all-nets), Encapsulation Mode (Tunnel), and IKE Config Mode (ConfigModePool). Below this, the 'Algorithms' tab is also visible, showing IKE Algorithms (High), IKE Life Time (28800 seconds), IPsec Algorithms (High), IPsec Life Time (3600 seconds), and IPsec Life Time (0 kilobytes).

Authentication

- Select Pre-shared Key
- Select the pre-shared key you created in step 3
- Local ID Type: Select Auto

XAUTH

- Select Require IKE Xauth user authentication for inbound IPsec tunnels

The screenshot shows the 'XAuth' tab in a configuration window. It has three radio buttons: 'Off', 'Require IKE XAuth user authentication for inbound IPsec tunnels' (which is selected), and 'Pass username and password to peer via IKE XAuth, if the remote gateway requires it.' Below these are three input fields labeled 'Username:', 'Password:', and 'Confirm Password:'.

Routing

- Automatic Routing: Check Dynamically add route to the remote network when a tunnel is established
- Use the defaults for the remaining settings

The screenshot shows the 'Automatic Routing' tab. It contains two checkboxes: 'Allow DHCP over IPsec from single-host clients' (unchecked) and 'Dynamically add route to the remote network when a tunnel is established' (checked).

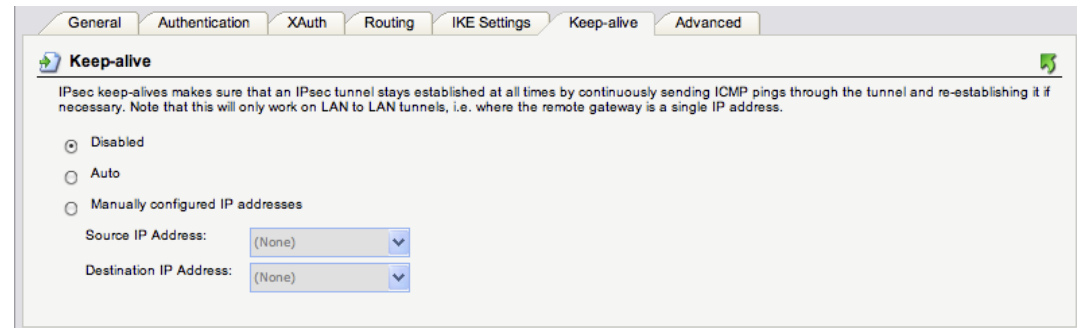
IKE Settings

- We will be using the default IKE settings as shown in the screenshot
- If you make any changes here, you will need to modify the settings in VPN Tracker's Advanced tab to match them

The screenshot shows the 'IKE Settings' tab with several sections: 'IKE' (Main selected, Aggressive with DH Group 2), 'Perfect Forward Secrecy' (PFS set to None, DH Group 2), 'Security Association' (Per Net selected), 'NAT Traversal' (On if supported and NATed selected), and 'Dead Peer Detection' (checked).

Keep-Alive

- We will be using the default keep-alive settings as shown in the screenshot



The screenshot shows the 'Keep-alive' tab in a configuration window. The tabs at the top are General, Authentication, XAuth, Routing, IKE Settings, Keep-alive, and Advanced. The 'Keep-alive' tab is selected. It contains a title bar with a green icon and the text 'Keep-alive'. Below the title bar is a paragraph of text: 'IPsec keep-alives makes sure that an IPsec tunnel stays established at all times by continuously sending ICMP pings through the tunnel and re-establishing it if necessary. Note that this will only work on LAN to LAN tunnels, i.e. where the remote gateway is a single IP address.' There are three radio buttons: 'Disabled' (selected), 'Auto', and 'Manually configured IP addresses'. Below the radio buttons are two dropdown menus: 'Source IP Address:' and 'Destination IP Address:', both showing '(None)'.

Advanced

- Uncheck the box **Add route for remote network**.
- **Important:** If you do not uncheck this box, you will cut off your D-Link from the network.
- Click **OK** to save the IPsec tunnel



The screenshot shows the 'Automatic Route Creation' tab in a configuration window. The tabs at the top are General, Authentication, XAuth, Routing, IKE Settings, Keep-alive, and Advanced. The 'Automatic Route Creation' tab is selected. It contains a title bar with a green icon and the text 'Automatic Route Creation'. Below the title bar is a paragraph of text: 'Automatically add route for remote network.' There is a checkbox labeled 'Add route for remote network' which is unchecked. Below the checkbox is a text field labeled 'Route Metric:' with the value '90' entered.

Step 5 – Add an XAUTH User

- Go to User Authentication > Local User Databases
- Click Add > Local User Database
- Name: Enter a name for the user database
- Click OK to save the database
- Click Add > User
- Username: Enter a name (4) for the user
- Password: Enter a password (5) for the user
- Click OK to add the user

The screenshot shows the 'User' configuration page. At the top, there's a header with a user icon and the title 'User'. Below the header, a sub-header states: 'User credentials may be used in User Authentication Rules, which in turn are used in e.g. PPP, IPsec XAuth, Web Authentication, etc'. The main content area has two tabs: 'General' (selected) and 'SSH Public Key'. The 'General' tab is divided into two sections. The first section, titled 'General', contains fields for 'Username:' (with the value 'alice'), 'Password:', 'Confirm Password:', and 'Groups:'. Below these fields is a help icon and the text 'Comma separated list of groups'. Further down, there are two lines of explanatory text: 'Users that are members of the 'administrators' group are allowed to change the firewall configuration.' and 'Users that are members of the 'auditors' group are only allowed to view the firewall configuration.' Below this text are two buttons: 'Add administrators' and 'Add auditors'. The second section, titled 'Per-user PPTP/L2TP IP Configuration', contains three fields: 'Static Client IP Address:' (a dropdown menu showing '(None)'), 'Networks behind user:' (a dropdown menu showing '(None)'), and 'Metric for networks:' (a text input field).

Step 6 – Add a User Authentication Rule

- Go to User Authentication > User Authentication Rules
- Click Add > User Authentication Rule

General

- **Name:** Enter a name for the authentication rule (e.g. VPN Tracker)
- **Agent:** Select XAUTH
- **Authentication Source:** Select Local
- **Originator IP:** Select all-nets

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

Name:	VPNTracker
Agent:	XAuth
Authentication Source:	Local
Interface:	(None)
Originator IP:	all-nets
Terminator IP:	(None)

Below the fields, there is a note: "For XAuth and PPP, this is the tunnel originator IP."

Authentication Options

- **Local User DB:** Select the database from step 5 (e.g. VPNTrackerUsers)
- All other settings are left at their default values.
- Click OK to add the authentication rule

The screenshot shows the 'Authentication Options' tab of the same configuration window. It contains the following elements:

- A heading: "Select one or more authentication servers. Also select the authentication method, which is used for encrypting the user password."
- A section for "Radius Server(s)" with two lists: "Available" and "Selected". There are buttons ">>" and "<<" between them, and "Move up" and "Move down" buttons below the "Selected" list.
- A "Radius Method:" dropdown menu set to "Unencrypted password".
- A "Local User DB:" dropdown menu set to "VPNTrackerUsers".

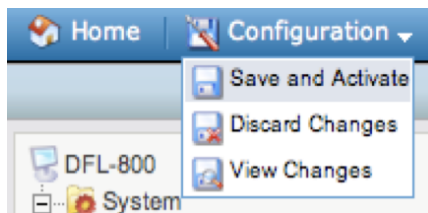
At the bottom right, there are "OK" and "Cancel" buttons.

Step 7 – Add an Access Rule

- Go to Rules > IP Rules
- Click Add > IP Rule Folder
- **Name:** Enter a name for the folder (e.g. VPNTracker)
- Click OK to add the new folder
- Click Add > IP Rule
- **Name:** Enter a name for the IP rule (e.g. VPNTracker)
- **Action:** Select Allow
- **Service:** Select the services that VPN users are allowed to access. In most cases, **all_tcpudpicmp** will be a suitable choice
- Address Filter
 - ◆ **Source Interface:** Select the IPsec tunnel interface created in step 4 (e.g. VPNTracker)
 - ◆ **Source Network:** Select the address book entry for your Mode Config IP addresses (e.g. ModeConfigAddresses)
 - ◆ **Destination Interface:** Select the lan interface
 - ◆ **Destination Network:** Select the lannet network
- Click OK to add the IP rule

The screenshot shows the 'IP Rule' configuration window. The title bar says 'IP Rule' with a subtitle 'An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.' There are tabs for 'General', 'Log Settings', 'NAT', 'SAT', 'SAT SLB', and 'Multiplex SAT'. The 'General' tab is active. It contains sections for 'General', 'Address Filter', and 'Comments'. In the 'General' section, 'Name' is 'VPNTracker', 'Action' is 'Allow', 'Service' is 'all_tcpudpicmp', and 'Schedule' is '(None)'. In the 'Address Filter' section, 'Source' has 'Interface' as 'VPNTracker' and 'Network' as 'ModeConfigAddresses'. 'Destination' has 'Interface' as 'lan' and 'Network' as 'lannet'. There is a 'Comments' text area at the bottom. 'OK' and 'Cancel' buttons are at the bottom right.

Important: Before being able to use your newly set up VPN tunnel, you will need to activate the configuration on the device: Click Configuration > Save and Activate, then follow the prompts to save and activate your configuration.

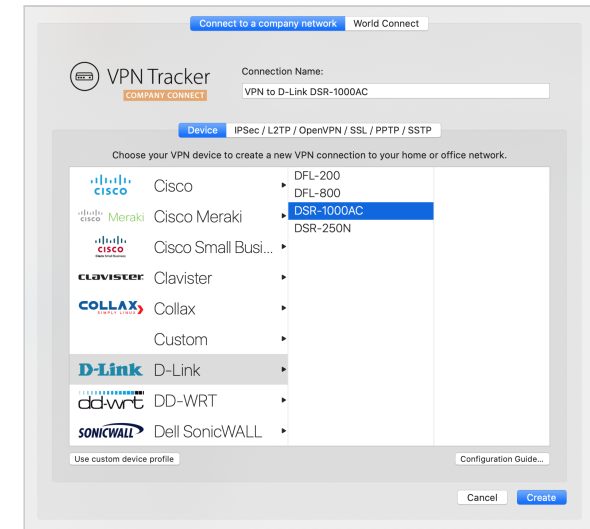


Task 2 – VPN Tracker Configuration

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

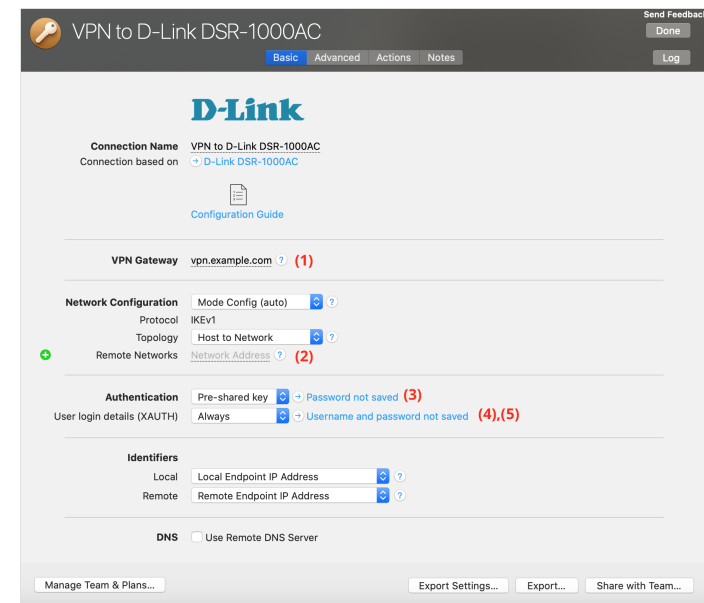
- Open VPN Tracker 365.
- Click on the + in the bottom left corner of the app window and select “Create new Company Connection”
- Select D-Link from the list.
- Select your model (e.g. DSR-1000AC) and enter a name for your connection.



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)**
- **Remote Networks:** Enter your device's LAN network **(2)**
- Under **Authentication**, enter the **Pre-Shared Key (3)** 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](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 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.