



# VPN Tracker 365

VPN Configuration Guide

**AWS Client VPN**

© 2019 equinux AG and equinux USA, Inc. All rights reserved.

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

The equinux logo is a trademark of equinux AG and equinux USA, Inc., registered in the U.S. and other countries. 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 manual is accurate. equinux is not responsible for printing or clerical errors.

Revised 13. May 2019

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

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

# Contents

<b>Introduction</b>	<b>4</b>
Using the Configuration Guide	4
Gateway Configuration	4
VPN Tracker Configuration	4
Scenario	4
Terminology	4
<b>My VPN Gateway Configuration</b>	<b>5</b>
<b>Device Configuration</b>	<b>6</b>
Set up for an existing VPN	6
Set up a new VPN Gateway	6
VPN Setup	6
Authentication	6
Aggressive Mode vs. Main Mode	6
Identifiers	7
Proposals (Phase 1 and Settings)	7
Local Endpoint (Network Access / Policy)	7
Remote Endpoint	7
VPN Gateway IP Address or Hostname	7
Login and Password	7
<b>VPN Tracker Configuration</b>	<b>8</b>
Add a connection	8
Configure the VPN connection for your device	9
<b>Testing the VPN connection</b>	<b>10</b>
<b>Troubleshooting</b>	<b>11</b>

# Introduction

This document describes how to set up a VPN connection using AWS Client VPN and VPN Tracker 365.

## Latest Documentation & Resources

AWS frequently updates their UI and configuration – please refer to the following AWS documents for additional information and more detailed steps.

[AWS VPN Client Walkthrough](#)

[AWS Client VPN Administrator Documentation](#)

## Prerequisites

The configuration described in this guide requires VPN Tracker 365. Make sure you have installed all available updates. The latest VPN Tracker updates can be downloaded from:

<https://www.vpntracker.com/download>

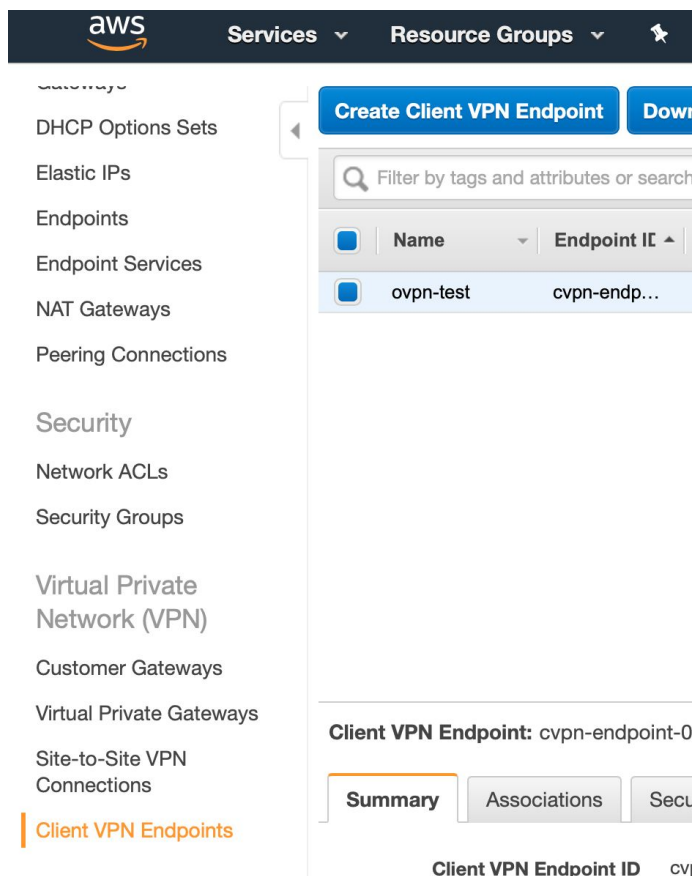
## Scenario

In our scenario we want to connect a Mac to your AWS infrastructure. We assume that the Mac running VPN Tracker already has an internet connection.

# Step 1: AWS Client VPN Setup

## Add a AWS Client VPN Configuration

- In your AWS Console, go to VPC and choose “Client VPN Endpoints”
- Then choose “Create Client VPN Endpoint”



### Basic Information

You'll be adding a new “VPN endpoint” – basically the VPN server VPN Tracker will be connecting to.

- Enter a name and description
- Enter the IP address range these users will be assigned (this shouldn't overlap with other common networks, e.g. your Office network, common home IP address ranges or the network range of your AWS infrastructure)

### Authentication

You have several options for authenticating your VPN users. We do not cover setting all options up here in detail – please [refer to the AWS documentation](#) if necessary.

- Choose an existing Server Certificate or create a new one
- Choose Active Directory or Certificate-based authentication for your users

### Note

For multiple users, Directory-based authentication is recommended. Users can simply sign in with a username and password, which is typically more familiar and easier to roll out than certificate-based authentication.

## Other Options

- Choose whether to enable optional logging
- Enter any DNS servers your users may require
- Choose UDP as a transport protocol for best performance

The screenshot shows the 'Create Client VPN Endpoint' page in the AWS Management Console. The breadcrumb trail is 'Client VPN Endpoints > Create Client VPN Endpoint'. The page title is 'Create Client VPN Endpoint'. Below the title, it says 'Create a new Client VPN endpoint to enable clients to access networks over a TLS VPN session'. The form has several sections: 'Name Tag' with a text input 'VPN Tracker 365 users'; 'Description' with a text input 'VPN access for our Mac users'; 'Client IP v4 CIDR\*' with a text input '192.168.60.0/24'; 'Authentication Information' with a 'Server certificate ARN\*' dropdown and 'Authentication Options' (radio buttons for 'Use Active Directory authentication' and 'Use mutual authentication'); 'Connection Logging' with a question 'Do you want to log the details on client connections?\*' and radio buttons for 'Yes' and 'No'; and 'Other optional parameters' with 'DNS Server 1 IP address' (8.8.8.8), 'DNS Server 2 IP address', and 'Transport Protocol' (radio buttons for 'TCP' and 'UDP'). At the bottom, there is a '\* Required' note, a 'Cancel' button, and a 'Create Client VPN Endpoint' button.

## Assign your VPN Endpoint to a VPC

You've created a new Client VPN Endpoint, now you need to tell AWS which virtual infrastructure (VPC) you want it to be able to access.

- In the overview, choose your Client VPN Endpoint
- Go to the "Associations" tab
- Click "Associate"
- Choose the VPC and subnets you want your VPN users to have access to

The screenshot shows the 'Create Client VPN Association to Target Network' page in the AWS Management Console. The breadcrumb trail is 'Client VPN Endpoints > Create Client VPN Association to Target Network'. The page title is 'Create Client VPN Association to Target Network'. Below the title, it says 'A Target Network is a subnet in a VPC. You associate a subnet in an Availability Zone to the Client VPN Endpoint. You can associate one subnet per Availability Zone. You can associate subnets in one VPC to a Client VPN Endpoint.' The form has a 'Client VPN Endpoint ID' dropdown with the value 'cvpn-endpoint-04530e6979a5557cb'. Below that, there is a 'VPC\*' dropdown and a 'Choose a subnet to associate\*' dropdown. At the bottom, there is a '\* Required' note, a 'Cancel' button, and an 'Associate' button.

## Note

You can also create a separate subnet for VPN users, which makes it easier to separate and monitor VPN traffic. Just make sure you create the subnet on the same VPC network.

## Add Authorization

Finally, you need to make sure your users have the right AWS permissions to access the VPC resources.

- In the overview, choose your Client VPN Endpoint
- Go to the “Authorization” tab
- Click “Authorize Ingress”

Then, on the next screen

- Enter the VPC network range your VPN users can access
- Choose whether to permit all users, or just selected AD groups

The screenshot shows the AWS Management Console interface for adding an authorization rule. At the top, the navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information 'thomas @ equinux' in Ireland. The breadcrumb trail is 'Client VPN Endpoints > Add authorization rule'. The main heading is 'Add authorization rule'. Below this, a sub-header states: 'Add authorization rules to grant clients access to the networks.' The form contains the following fields: 'Client VPN Endpoint ID' with the value 'cvpn-', 'Destination network to enable' with the value '192.168.10.0/24', 'Grant access to:' with two radio button options ('Allow access to all users' is selected, and 'Allow access to users in a specific Active Directory group' is unselected), and 'Description' with the text 'Give all VPN users access to our main VPC network.' At the bottom left, there is a note '\* Required'. At the bottom right, there are two buttons: 'Cancel' and 'Add authorization rule'.

### Tip

If you enter “0.0.0.0/0” as your network range, a user’s entire internet traffic will go through your VPN. Typically you’ll want to enter the specific network range your VPC is using though.

## Step 2: Configuring VPN Tracker 365

### Download the AWS Client VPN Configuration

Now you've configured your VPN on AWS, you can download a ready-made configuration file with settings for VPN Tracker 365.

- Go to the AWS Client VPN overview
- Choose your VPN Endpoint
- Click "Download Client Configuration"

### Add the Configuration to VPN Tracker 365

- Make sure you have the [latest version of VPN Tracker 365](#)
- Drag the Configuration file onto the VPN Tracker dock icon or
- Choose File > Import and select the "downloaded-client-config.ovpn" file

The screenshot shows the configuration interface for a VPN connection named "downloaded-client-config-2". The interface has tabs for "Basic", "Advanced", "Actions", and "Notes".

**Connection Name:** downloaded-client-config-2  
Connection based on: [Custom OpenVPN](#)

**Reload configuration:** Drop OpenVPN configuration file here

[Configuration Guide](#)

**VPN Gateway:** cvpn-endpoint-example.prod.clientvpn.eu-west-1.amazonaws.com  
**Port Number:** 443

**Network Configuration:**  
Push/Pull: ☐ ?  
Protocol: OpenVPN  
Topology: Host to Network ?

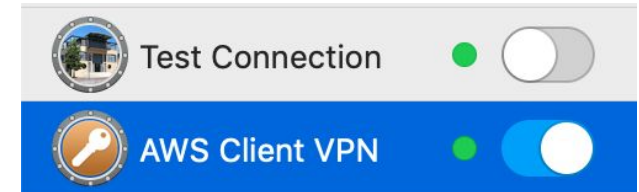
**Additional Remote Networks:** [Optional Network Address](#) ?



## Testing the VPN connection

### Connect to your VPN

- Check first of all that your internet connection is working as it should be.  
Use this link as a test: <https://www.vpntracker.com>
- Start the VPN Tracker 365 app.
- Click on the On/Off slider to turn on your connection.
- Depending on your setup, you will be prompted to enter your username and password.



### Tip

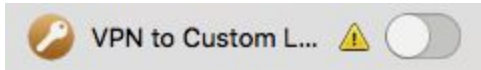
If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection.

### 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 and give you some troubleshooting steps to try.

**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](https://www.vpntracker.com/support) contains detailed troubleshooting advice. Answers to frequently asked questions (FAQs) can be found at: <https://www.vpntracker.com/support>

## Technical Support

If you're stuck, the technical support team at equinux is here to help. Contact us via <https://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).
- The manufacturer, the exact device model and the firmware version running on it.
- Screenshots of what you have configured on your VPN gateway, in particular all VPN-related settings.
- Screenshots of the VPN settings on your device