equinux

VPN Tracker 365

VPN Configuration Guide

AWS Client VPN

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

www.vpntracker.com

Contents

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

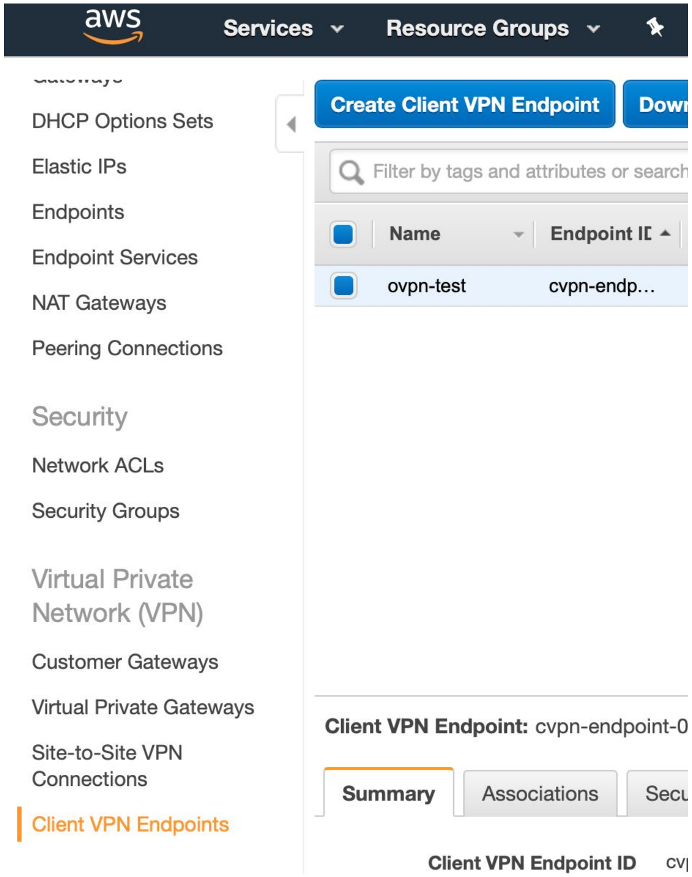
Scenario

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.

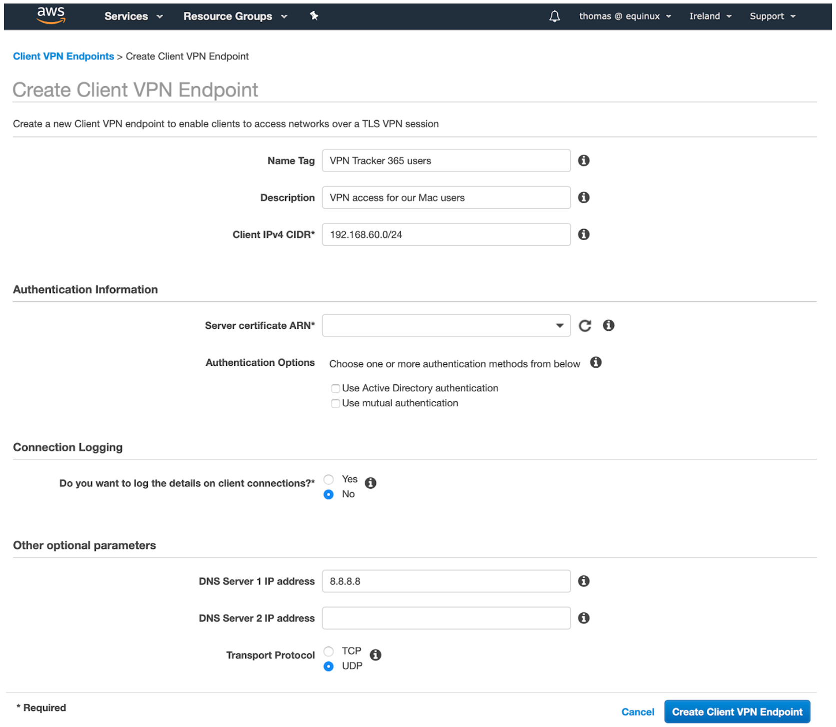
- ➔ Choose an existing Server Certificate or create a new one
- ➔ Choose Active Directory or Certificate-based authentication for your users

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



Client VPN Endpoints > Create Client VPN Endpoint

Create Client VPN Endpoint

Create a new Client VPN endpoint to enable clients to access networks over a TLS VPN session

Name Tag: VPN Tracker 365 users

Description: VPN access for our Mac users

Client IPv4 CIDR*: 192.168.60.0/24

Authentication Information

Server certificate ARN*:

Authentication Options: Choose one or more authentication methods from below

□ Use Active Directory authentication
□ Use mutual authentication

Connection Logging

Do you want to log the details on client connections?*: ○ Yes ● No

Other optional parameters

DNS Server 1 IP address: 8.8.8.8

DNS Server 2 IP address:

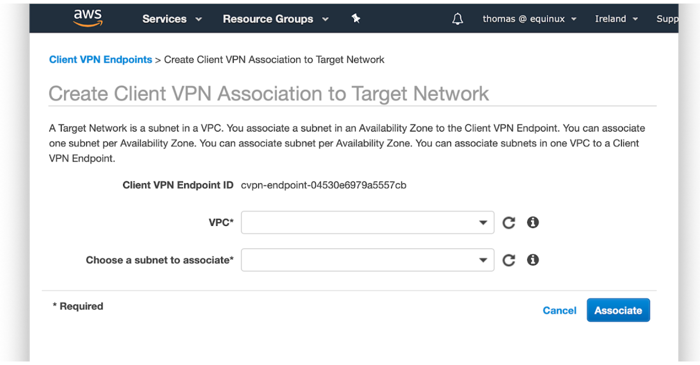
Transport Protocol: ○ TCP ● UDP

* Required

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



Client VPN Endpoints > Create Client VPN Association to Target Network

Create Client VPN Association to Target Network

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 subnet per Availability Zone. You can associate subnets in one VPC to a Client VPN Endpoint.

Client VPN Endpoint ID: cvpn-endpoint-04530e6979a5557cb

VPC*:

Choose a subnet to associate*:

* Required

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.

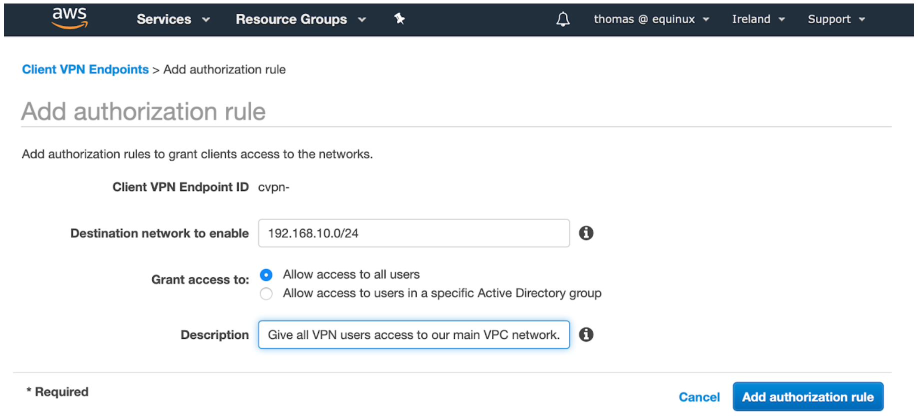
Add Authorization

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



Add authorization rule

Add authorization rules to grant clients access to the networks.

Client VPN Endpoint ID cvpn-

Destination network to enable 192.168.10.0/24

Grant access to: ● Allow access to all users
○ Allow access to users in a specific Active Directory group

Description Give all VPN users access to our main VPC network.

* Required

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

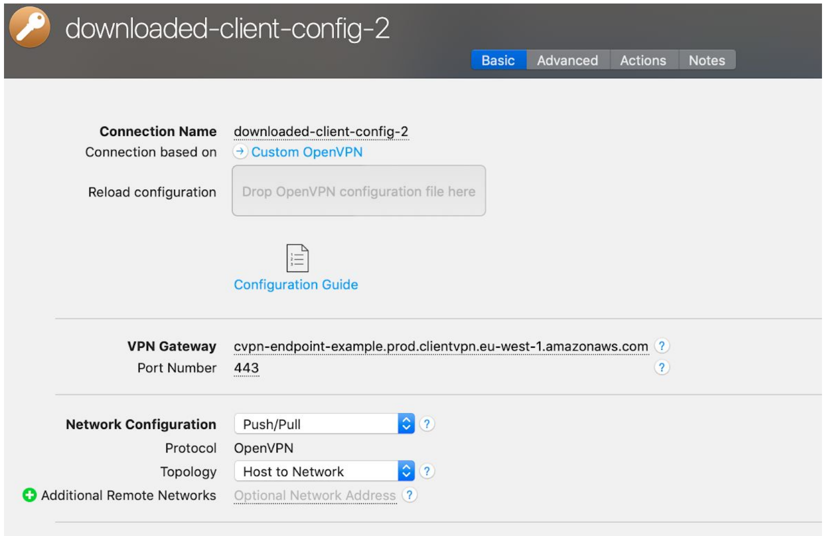
Download the AWS Client VPN Configuration

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



Connection Name: downloaded-client-config-2
Connection based on: Custom OpenVPN
Reload configuration: Drop OpenVPN configuration file here

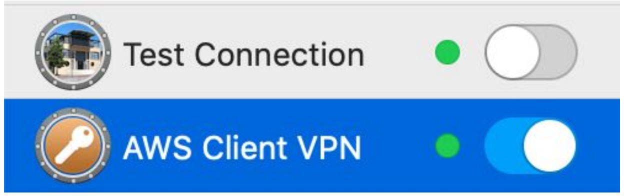
VPN Gateway: cvpn-endpoint-example.prod.clientvpn.eu-west-1.amazonaws.com
Port Number: 443

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

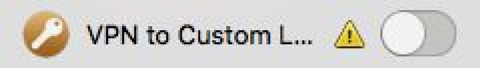
If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection.

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 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