equinux

VPN Tracker 365

VPN Configuration Guide

Cisco Meraki

MX Series

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 November 2020

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 WatchGuard Firebox VPN gateway device.

IP Addresses

(1) Cisco WAN IP Address: ______.______.______.______ (or host name ________________________________)

(2) LAN Network: ______.______.______.______ / ______.______.______.

Authentication

(3) Pre-Shared Key: ______________________

(4) XAUTH Username: ______________________

(5) XAUTH Password: ______________________

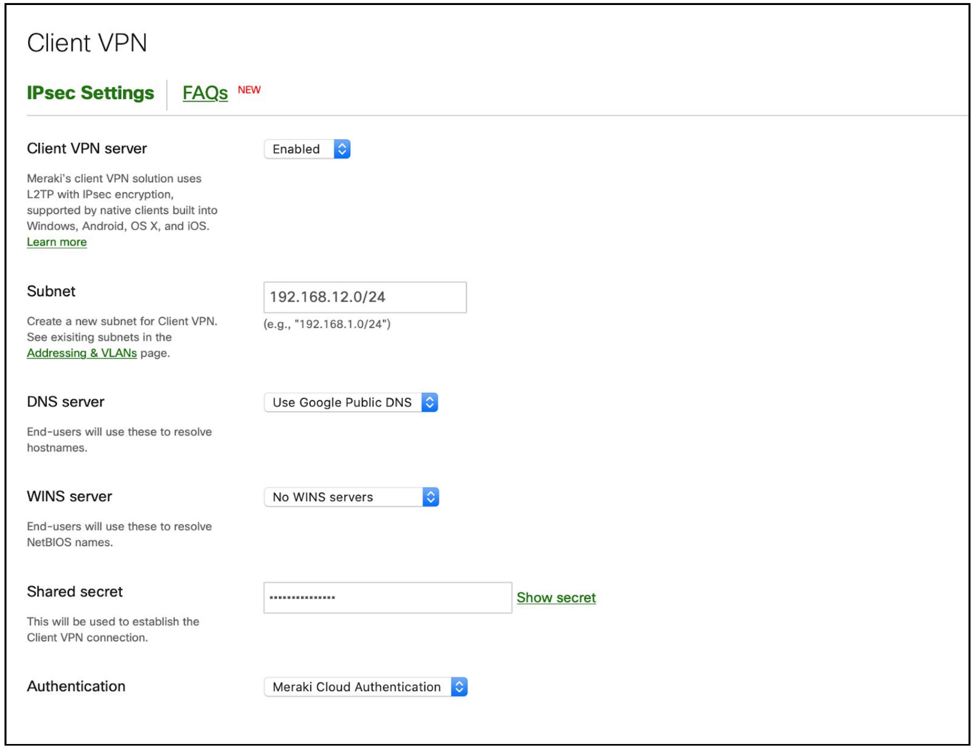
Task 1 – VPN Gateway Configuration

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 – Enable VPN on your Cisco Device

This step is only required if your Cisco device has not already been set up. If you have set up your device already, you can skip straight to step 2.

- ➔ Go to **Security & SD-WAN > Client VPN**.
- ➔ Set **"Client VPN Server"** to.**"Enabled"**
- ➔ Enter a "**Subnet"** for client VPN and make a note of it as **(2)** on your checklist
- ➔ Enter a secure **"Shared secret" and make a note of it as (3)** on your checklist
- ➔ Click "**Save**"



Client VPN

Client VPN server: Enabled

Meraki's client VPN solution uses L2TP with IPsec encryption, supported by native clients built into Windows, Android, OS X, and iOS. Learn more

Subnet: 192.168.12.0/24 (e.g., "192.168.1.0/24")

Create a new subnet for Client VPN. See exisiting subnets in the Addressing & VLANs page.

DNS server: Use Google Public DNS

End-users will use these to resolve hostnames.

WINS server: No WINS servers

End-users will use these to resolve NetBIOS names.

Shared secret: ················ Show secret

This will be used to establish the Client VPN connection.

Authentication: Meraki Cloud Authentication

Step 2 – Retrieve Network Settings

WAN IP or Host Name

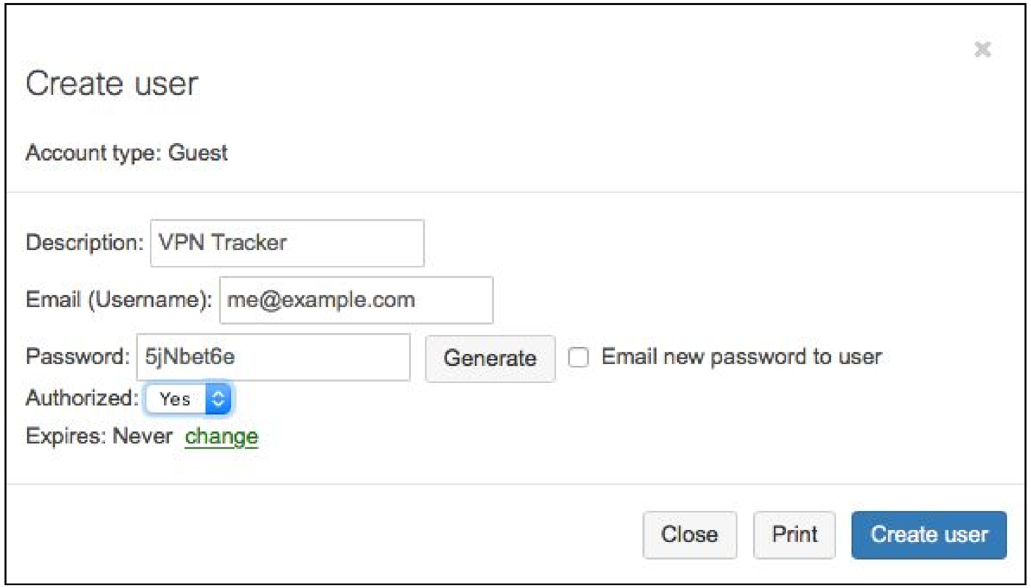
- ➔ Connect to your Meraki's web interface.
- ➔ Go to **Security & SD-WAN** > **Appliance Status**.
- ➔ Write down the **WAN address or Hostname as (1)** on your checklist

LAN Network

- ➔ **Go to Security & SD-WAN > Route table**
- ➔ Write down the **Local LAN** as **(2)** on your checklist (skip this step if already entered in step 1)

Step 3 – Add a VPN User

- ➔ Go to **Security appliance > Client VPN**
- ➔ Click „**Add new user**"
- ➔ Enter an **Email address (Username)** **(4)** and **Password** **(5)** for your user
- ➔ Select **"Authorized > Yes"**



Create user

Account type: Guest

Description: VPN Tracker

Email (Username): me@example.com

Password: 5jNbet6e

Authorized: Yes

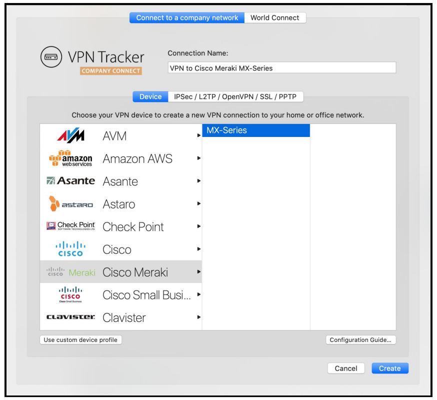
Expires: Never change

Task 2 – VPN Tracker Configuration

After finishing task 1, you should now have a completed a configuration checklist containing your Cisco Meraki MX firewall's settings. We will now create a matching configuration in VPN Tracker 365.

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 Cisco Meraki from the list.
- ➔ Select MX Series and enter a name for your connection.



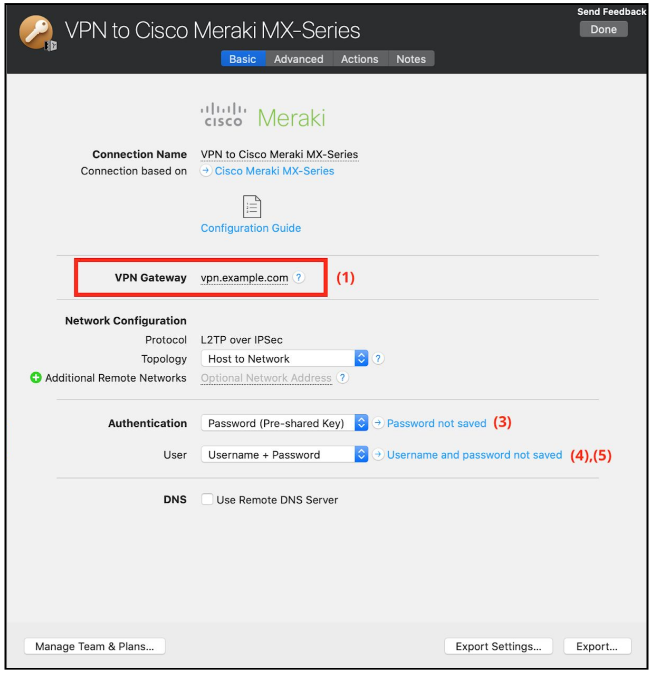
Connection Name: VPN to Cisco Meraki MX-Series

Choose your VPN device to create a new VPN connection to your home or office network.

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 Public IP address (or hostname) of your device that you wrote down as **(1)**. If the device has a DNS host name (e.g. vpn.example.com), use that instead.
- ➔ Network configuration: Leave as "Host to Network"
- ➔ Authentication: Here you can enter the Shared Secret **(3)** and username **(4)** and password **(5)** you configured during the Cisco setup. Save these in your Keychain so VPN Tracker 365 remembers them.



VPN to Cisco Meraki MX-Series

Connection Name: VPN to Cisco Meraki MX-Series
Connection based on: Cisco Meraki MX-Series

VPN Gateway: vpn.example.com (1)

Network Configuration
Protocol: L2TP over IPSec
Topology: Host to Network
Additional Remote Networks: Optional Network Address

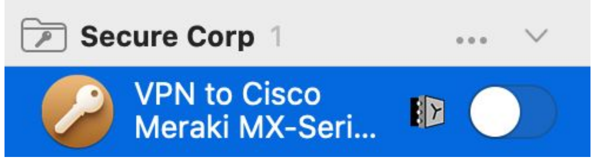
Authentication: Password (Pre-shared Key) Password not saved (3)
User: Username + Password Username and password not saved (4),(5)

DNS: □ Use Remote DNS Server

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:

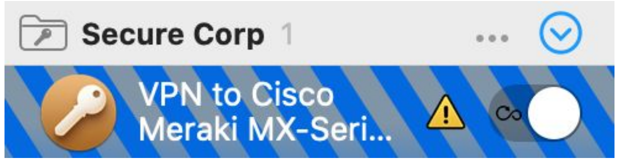
If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection. Wait for the test to complete.

- ➔ Depending on your setup, You will be prompted to enter your pre-shared key **(3)** and your XAUTH username **(4)** and password **(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


Secure Corp 1

VPN to Cisco Meraki MX-Seri...

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.