01/06/2020

TC Router 4G LTE and mGuard Secure VPN Client VPN Configuration Guide

1 Description

This application note describes how you can establish a VPN connection from the mGuard Secure VPN Client to the TC Router 4G LTE. This requires the use of certificates.

You need the following:

Name	Order No.	Description
MGUARD SECURE VPN CLIENT LIC	2702579	License for mGuard Secure VPN Client
TC Router 3002T-4G	2702528 (EU) 2702532 (VZW) 2702533 (ATT)	4G LTE cellular modem.
SIM Card with public/static IP address	Contact cellular provider	Active SIM card with public/static IP address that enables the TC Router to connect to the Internet.

WARNING:
This application note does **not** replace the device-specific documents.
Please follow the safety notes in the associated package slips, data sheets, and user manuals.

Make sure you always use the latest documentation.
It can be downloaded at phoenixcontact.net/products.

Table of Contents

2 Certificates

Learn how to create certificates in the “Quick Reference Guide for creating certificates” at phoenixcontact.com/product/2314008.

Certificates required

For a VPN tunnel in connection with the mGuard Secure Client, you require three certificates: a private certificate from each side and a public certificate from the client loaded in the VPN server.

- Machine certificate.p12#
- Client certificate.p12#
- Client certificate.crt

3 Configuring the router

3.1 Mobile communication router

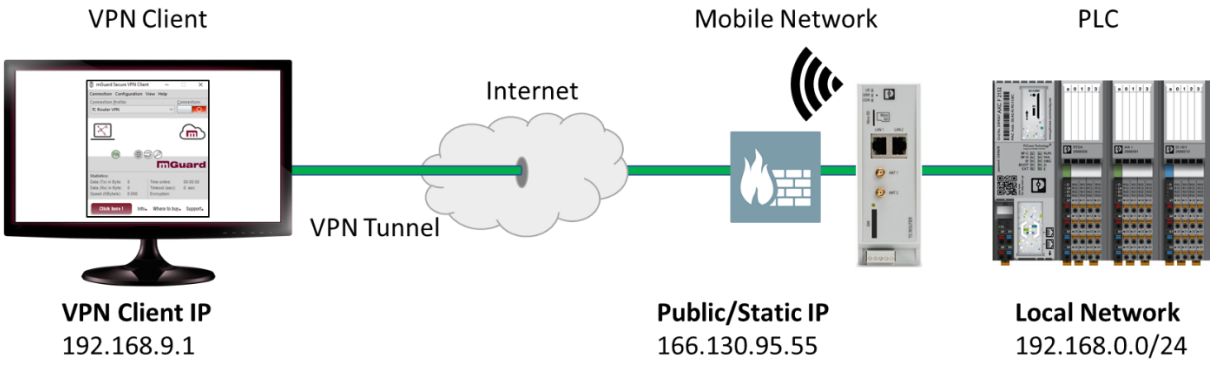

Figure 1 System overview with mobile router

Ensure that the TC Router has an active data plan with a public/static IP address. Please check with your cellular provider to learn more about the data plan associated with the SIM card

- Power up the TC Router and connect to the Internet
  - Refer to the TC Router user manual for setup instructions
- Open the web-based management. Log in with your username and password.
  - Default IP address: 192.168.0.1
  - Default username: admin
  - Default password: admin
- Switch to the “VPN >> IPsec >> Certificates” sub-folder.
- Load the Client certificate.crt and Machine certificate.p12# into the TC Router
- Confirm with “Apply”

Figure 2 IPsec certificates

- Switch to the “VPN >> IPsec >> Connections” sub-folder.
- Enter a name for the VPN connection.
- Confirm with “Apply”.
- Under the “Settings” main item, click on the “Edit” button.

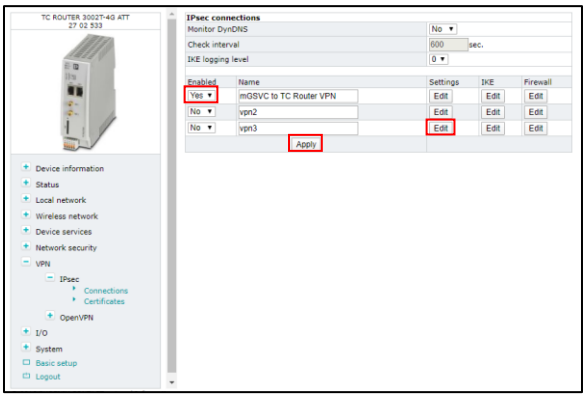

Figure 3 IPsec connections

- Activate the VPN tunnel.
- Select the certificates.
- Enter the network area of the local network. Enter the fixed IP address of the client. The example shows the network area 192.168.0.0/24 and for the client 192.168.9.1/32.
- Enable remote masquerading
- Confirm with “Apply”.

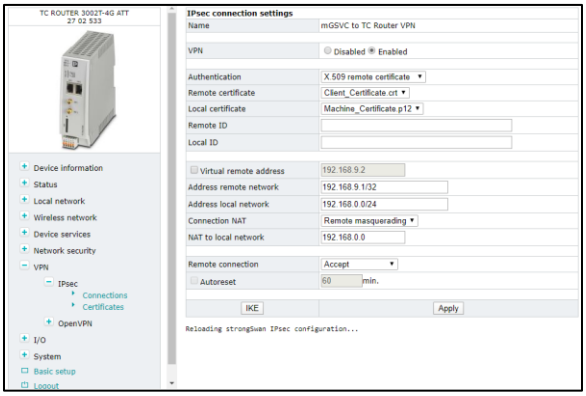

Figure 4 IPsec connection settings

- Click on “IKE”
- Take the settings from the figure below.

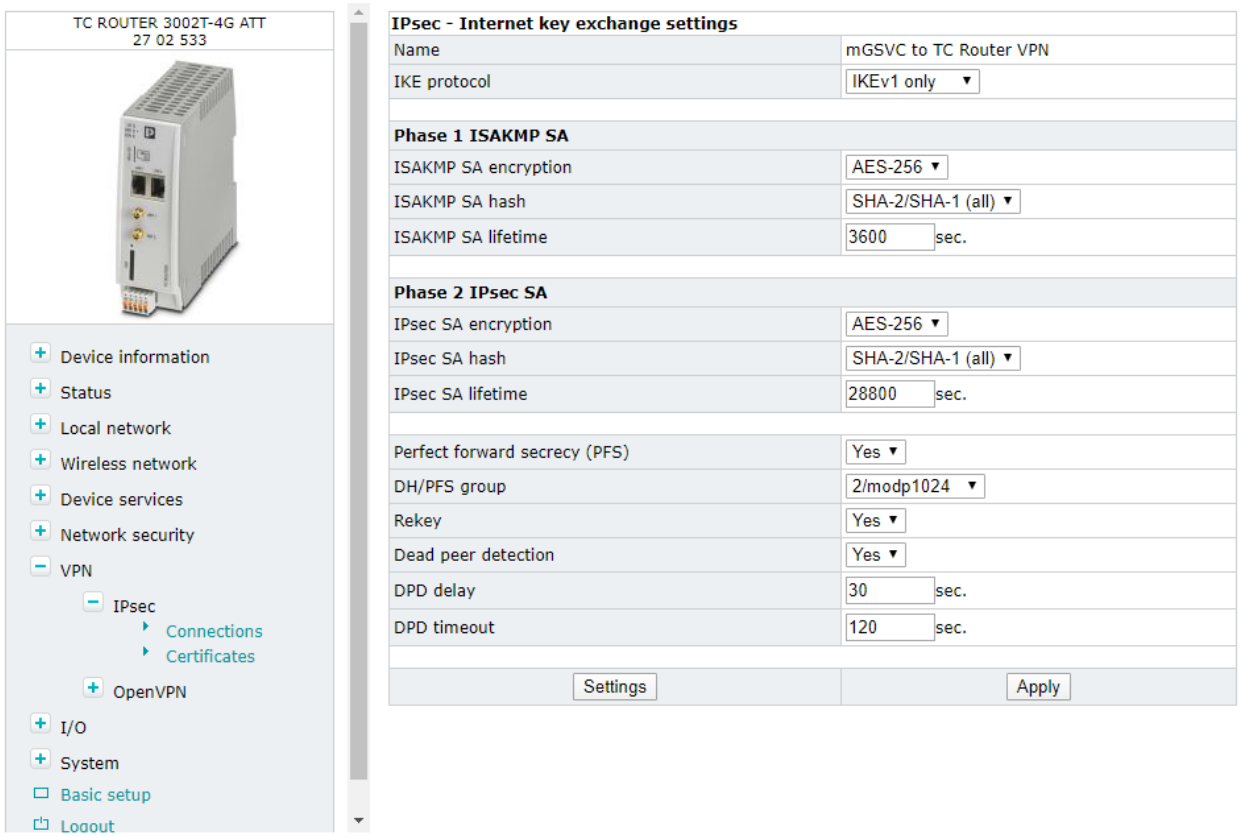

Figure 5 IPsec – Internet key exchange settings

The settings for the TC Router are now complete

In the “Status >> IPsec status” stub-folder you can monitor the status of the VPN tunnel.

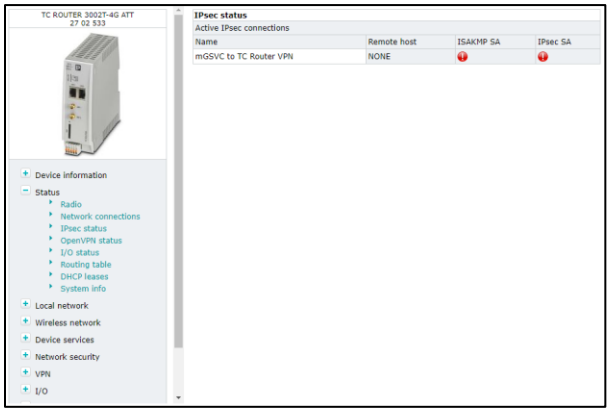

Figure 6 IPsec connection status menu

4 Configuring the mGuard Secure VPN Client

4.1 Installation

- Install the mGuard Secure VPN Client as described in the corresponding data sheet (see phoenixcontact.com/ product/2702579).

4.2 Uploading a certificate

- Start the mGuard Secure VPN Client software
- Navigate to “Configuration >> Certificates”
- Select “Add” and name the certificate “Client Certificate”
- In the “User Certificate” tab, select the “from PKCS#12 file” option.
- Upload the previously created Client Certificate.p12#

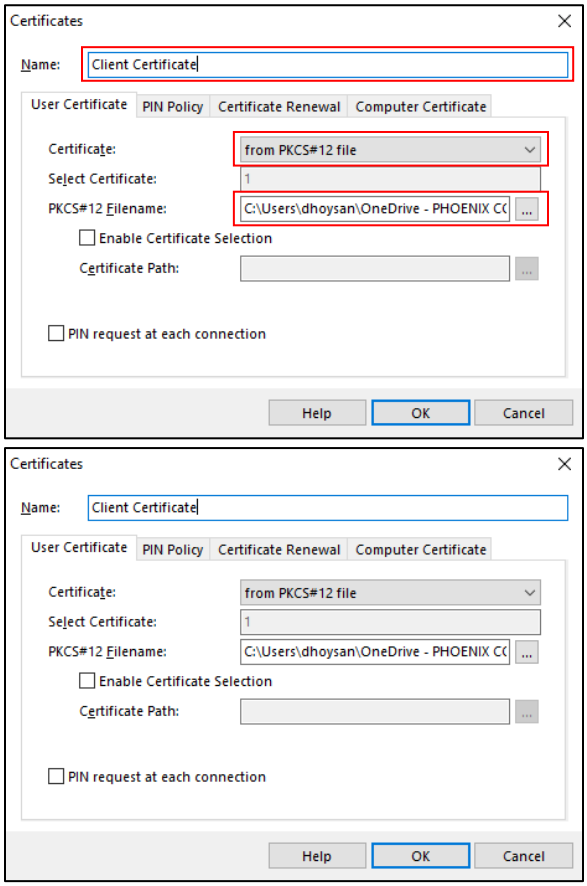

Figure 7 mGSVC certificate upload

4.3 Creating a profile

- In the main menu, select “Configuration >> Profiles”.
- Add a new profile

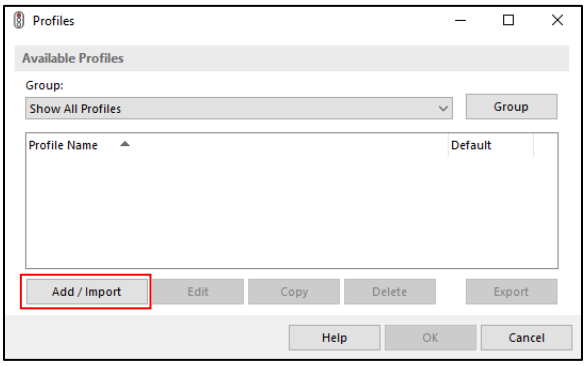

Figure 8 Add mGSVC configuration profile

- Select the manual configuration
- Enter a profile name

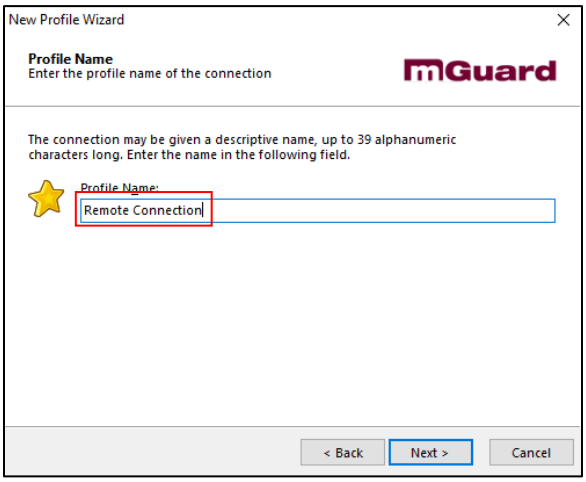

Figure 9 Profile name

- Select the previously uploaded certificate
- Click next

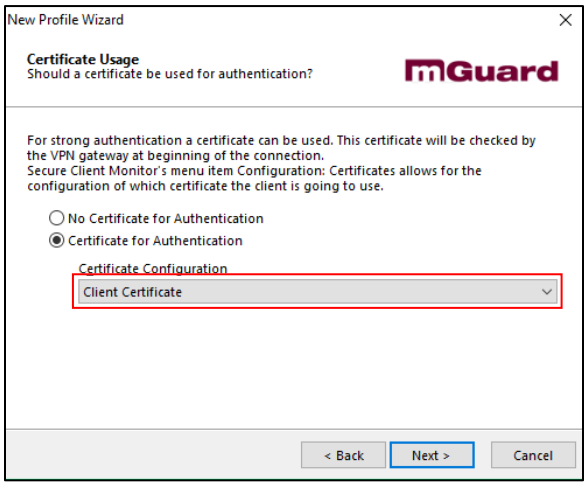

Figure 10 Certificate Configuration

- In “Gateway”, enter the public/static IP address address of the remote station. In this example the address is 166.130.95.55
- Click next

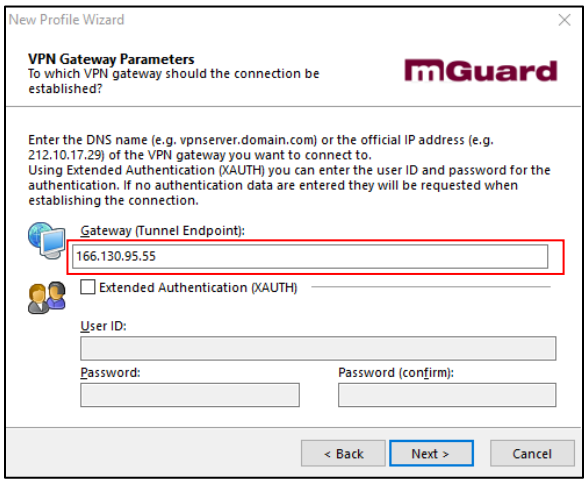

Figure 11 Gateway (Tunnel Endpoint)

- Apply the IPsec parameters shown below:
  - Main mode
  - DH2 (modp1024)

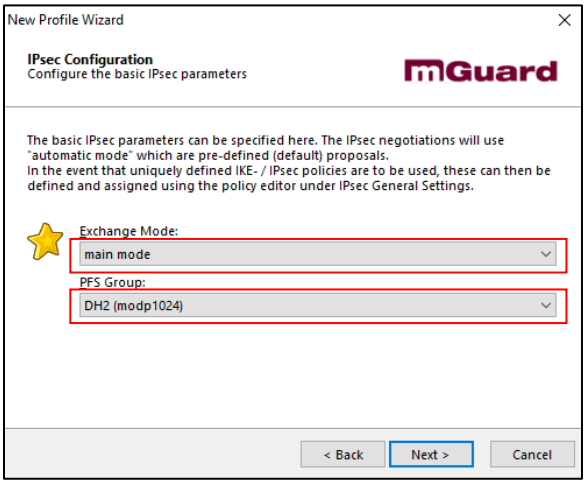

Figure 12 IPsec Configuration

- Leave the ASN1 Distinguished Name ID field blank. This should only be used in configurations requiring a Pre-shared key instead of certificates

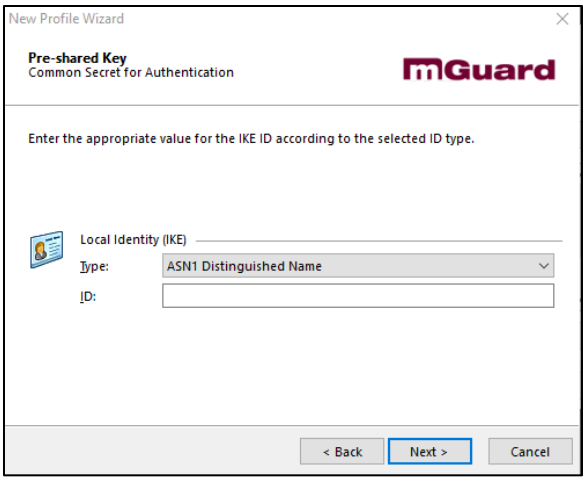

Figure 13 Pre-shared Key

- Enter the VPN client IP address. In the example in the system overview, the IP address is 192.168.9.1

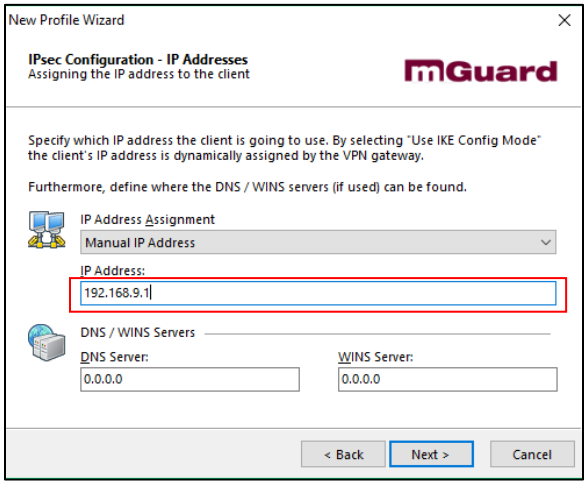

Figure 14 IPsec Configuration – Client IP Address

- Enter the network area of the remote station. In the example in the system overview, the network area is 192.168.0.0/24

NOTE: Malfunction

The logical network on the PC and on the remote station must be located in different network areas. Otherwise problems may arise when routing.

– Select different network areas.

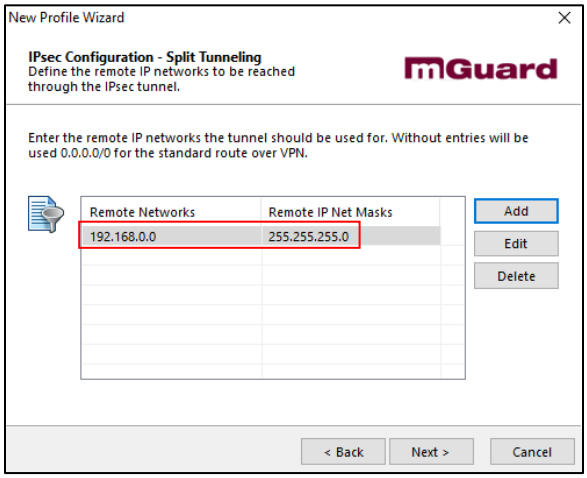

Figure 15 IPsec Configuration – Remote Network

- Close the wizard with “Finish”

- From the VPN Client main menu, select “Configuration >> Profiles”
- Select the Remote Connection profile and choose edit

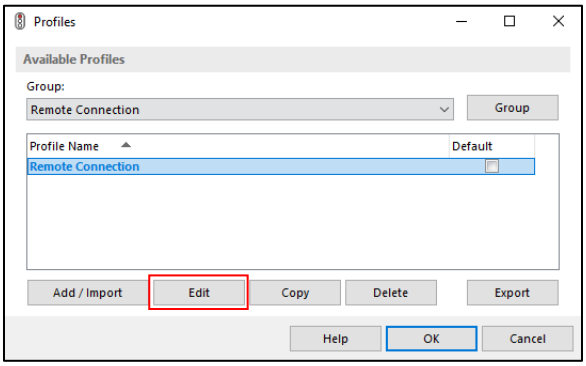

Figure 16 Edit the configuration

- Select “Line Management” from the menu and set the Inactivity timeout to 0 seconds to prevent any timeout issues.

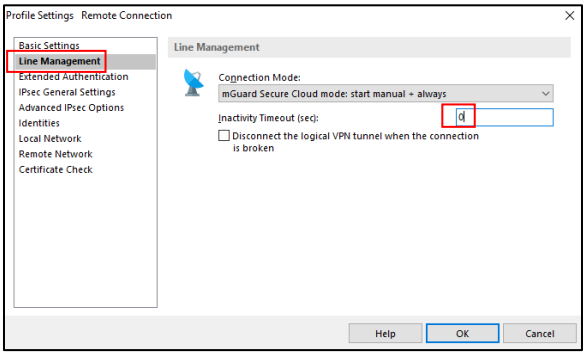

Figure 17 Inactivity Timeout

- Select “IPsec General Settings” from the menu, and set IKE Policy and IPsec Policy to “All algorithm”

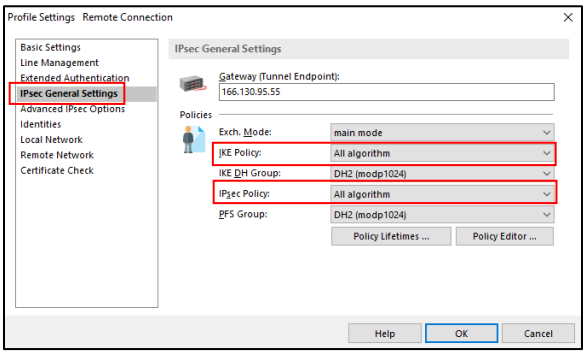

Figure 18 IKE Policy and IPsec Policy

Exit the menu. The VPN Client software setup is now complete

4.4 Testing the connection

- In the main menu, select your profile.
- Activate the connection by clicking the connection slider

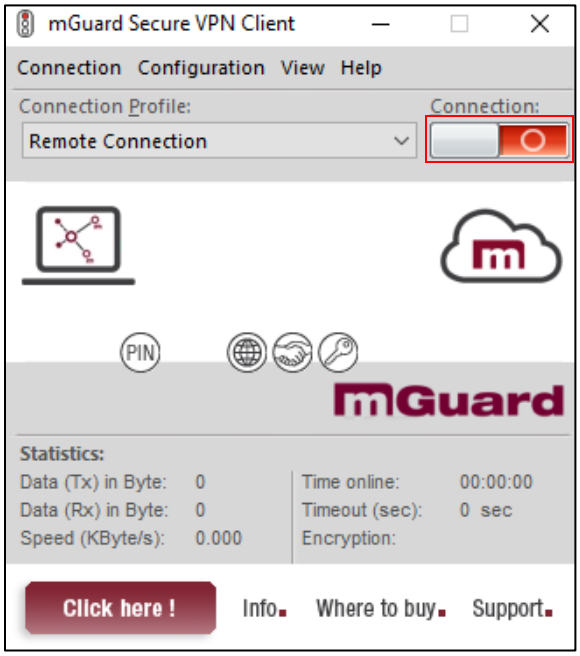

Figure 19 Testing the connection

- The VPN client will prompt you for a PIN. This is the password associated to the p12 certificate. Enter this password to establish the connection

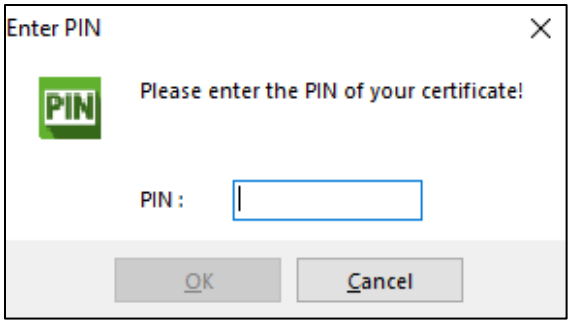

Figure 20 Entering the password

The connection is established when all four circles and the tunnel turn green as shown below.

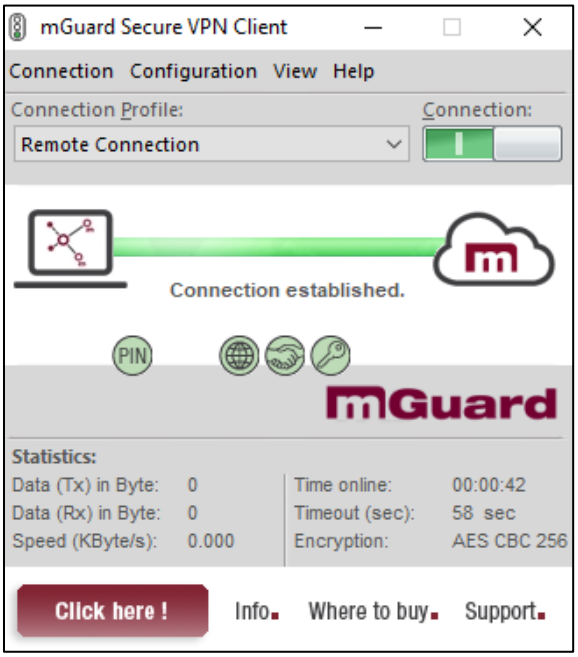

Figure 21 Connection established

- Verify the tunnel has been established by logging into the TC Router and navigating to “Status >> IPsec status”. A successful connection will show two green check marks

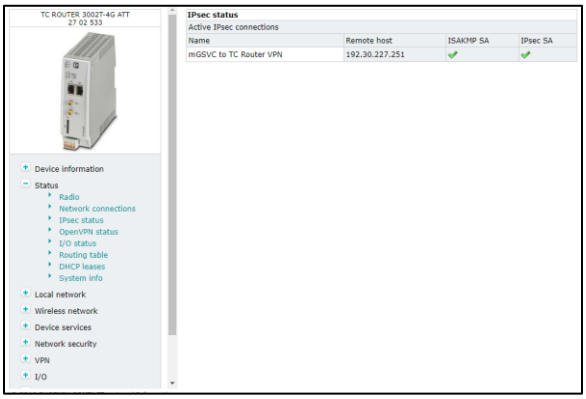

Figure 22 Connection verification

Congratulations, you have successfully established a VPN tunnel between the mGuard Secure VPN Client software on your laptop to a TC Router over the cellular network.