

***DrayTek***

*VPN*

***Remote Dial-IN***

***DrayTek Smart VPN Client***



## Inhoudsopgave

VPN Remote Dial In.....	3
Verbinding maken met de DrayTek router .....	4
DrayTek VPN Remote Dial In configuratie – PPTP VPN .....	5
PPTP VPN verbinding via Smart VPN Client.....	8
DrayTek VPN Remote Dial In configuratie – IPSec VPN .....	13
IPSec VPN verbinding via Smart VPN Client .....	16
DrayTek VPN Remote Dial In configuratie – L2TP over IPSec VPN.....	19
L2TP over IPSec VPN verbinding via Smart VPN Client .....	22
DrayTek VPN Remote Dial In configuratie – SSL VPN .....	24
SSL VPN verbinding via Smart VPN Client.....	27

## VPN Remote Dial In

Met een Virtual Private Network (VPN) is het mogelijk om door 3tanda van een beveiligde (geautoriseerd en/of versleuteld) verbinding te communiceren met een lokaal netwerk via het Internet.

Een VPN-verbinding kan ook gebruikt worden om twee 3tanda netwerken met elkaar te verbinden. DrayTek verdeelt VPN-verbindingen in twee categorieën.

### 1. Remote Dial-In

De verbinding wordt opgebouwd door een enkele computer of client. Deze krijgt toegang tot het 3tanda netwerk van de DrayTek.

### 2. LAN-to-LAN

Een LAN-to-LAN verbinding wordt opgebouwd tussen twee routers. Beide 3tanda netwerken worden met elkaar verbonden. Hierdoor kunnen alle computers binnen de 3tanda netwerken verbinding maken met het andere netwerk.

In deze handleiding leggen we aan u uit hoe u een **Remote Dial-In VPN** verbinding kunt realiseren naar een DrayTek product. Hierbij zullen we de volgende VPN type bespreken:

**PPTP** (Point-to-Point Tunneling Protocol)

**IPSEC** (Internet Protocol Security)

**SSL** (Secure Socket Layer)

**L2TP** (Layer Two Tunneling Protocol)

Op de computer of client maken we gebruik van de Windows VPN client of van de gratis te downloaden **DrayTek Smart VPN Client**. De Smart VPN Client is gratis te downloaden op onze [www.draytek.nl](http://www.draytek.nl) website.

## Verbinding maken met de DrayTek router

In uw webbrowser gaat u naar het default IP-adres van de DrayTek, dit is <http://192.168.1.1>.

Een loginscherm van de DrayTek zal verschijnen waar u op basis van een gebruikersnaam en wachtwoord kunt inloggen.

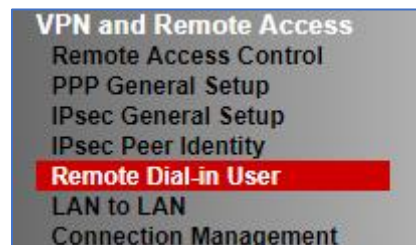


The image shows a login interface for a DrayTek Vigor2133 Series router. At the top left is the DrayTek logo in red. To its right, a red banner contains the text "Vigor2133 Series" in white. Below this, a black banner with the word "Login" in white is positioned on the left. The main area is white and contains two input fields: "Username" and "Password". Below the password field is a grey "Login" button. At the bottom, a small copyright notice reads "Copyright © 2000-2018 DrayTek Corp. All Rights Reserved."

U komt in het hoofdmenu van de DrayTek terecht.

## DrayTek VPN Remote Dial In configuratie – PPTP VPN

In het menu gaat u naar VPN and Remote Access om vervolgens te klikken op Remote Dial In User.



U komt op een overzichtsscherm terecht waarin nog geen actieve profielen staan. Door een nieuw profiel aan te maken klikt u op het juiste index nummer.

VPN and Remote Access >> Remote Dial-in User

Remote Access User Accounts: | [Set to Factory Default](#) |

Index	Enable	User	Status	Index	Enable	User	Status
<u>1.</u>	<input type="checkbox"/>	???	---	<u>17.</u>	<input type="checkbox"/>	???	---
<u>2.</u>	<input type="checkbox"/>	???	---	<u>18.</u>	<input type="checkbox"/>	???	---
<u>3.</u>	<input type="checkbox"/>	???	---	<u>19.</u>	<input type="checkbox"/>	???	---
<u>4.</u>	<input type="checkbox"/>	???	---	<u>20.</u>	<input type="checkbox"/>	???	---
<u>5.</u>	<input type="checkbox"/>	???	---	<u>21.</u>	<input type="checkbox"/>	???	---
<u>6.</u>	<input type="checkbox"/>	???	---	<u>22.</u>	<input type="checkbox"/>	???	---
<u>7.</u>	<input type="checkbox"/>	???	---	<u>23.</u>	<input type="checkbox"/>	???	---

Bij het configureren van een PPTP Remote Dial In profiel zijn onderstaande instellingen van belang:

- Enable this Account:** Door hier een vinkje te zetten activeert u het VPN profiel.
- Idle Timeout:** Deze optie staat standaard op 300 seconden, dit betekent dat de DrayTek de VPN verbinding zal verbreken indien er 5 minuten geen activiteit plaatsvindt. U kunt deze optie eventueel op 0 seconden zetten, zodoende zal de DrayTek hierop geen controle meer uitvoeren.
- Allowed Dial In Type:** Selecteer het juiste VPN Protocol wat u wilt gebruiken. In dit geval selecteert u PPTP.
- Specify Remote Node:** Hier geeft u het publieke IP-adres op van de remote client, aan de hand van dit IP-adres voert de DrayTek een beveiligingscontrole uit. Indien dit IP-adres niet bekend is of telkens verschillend is hoeft u deze instelling niet op te geven. In dat geval hoeft u deze optie niet in te schakelen.
- Username/Password:** Geef hier de juiste gebruikersnaam/wachtwoord gegevens op voor het VPN account.

**Subnet:** Indien u gebruik maakt van meerdere LAN subnetten kunt u hier aangeven in welk LAN subnet deze VPN gebruiker moet komen wanneer een verbinding wordt opgezet.

Onderstaande afbeelding geeft een voorbeeld configuratie aan, deze kunt u natuurlijk naar uw eigen wens inrichten.

The screenshot displays a configuration window titled "Index No. 3" with two main columns of settings. The left column is titled "User account and Authentication" and includes: "Enable this account" (checked), "Idle Timeout" set to 300 seconds, "Allowed Dial-In Type" with "PPTP" selected, "Specify Remote Node" (unchecked), "Remote Client IP" and "or Peer ID" fields, "Netbios Naming Packet" set to "Pass", "Multicast via VPN" set to "Block", and "Subnet" set to "LAN 1". The right column is titled "Authentication Method" and includes: "Username" set to "draytek", "Password" field, "Enable Mobile One-Time Passwords(mOTP)" (unchecked), "IKE Authentication Method" set to "Pre-Shared Key" with a "Max: 64 characters" limit, "Digital Signature(X.509)" set to "None", "IPsec Security Method" set to "Medium(AH)", "High(ESP)" with "DES", "3DES", and "AES" all checked, and a "Local ID (optional)" field.

Dit zijn de basis instellingen welke belangrijk zijn voor het opzetten/instellen van een VPN Remote Dial In User op basis van PPTP.

Nu kunt u er bijvoorbeeld ook voor kiezen om elke VPN gebruiker een vast IP-adres te geven. Dit kunt u doen door een vinkje te zetten bij Assign Static IP Address.

**Subnet**  
LAN 1 ▾  
 Assign Static IP Address  
192.168.1.250

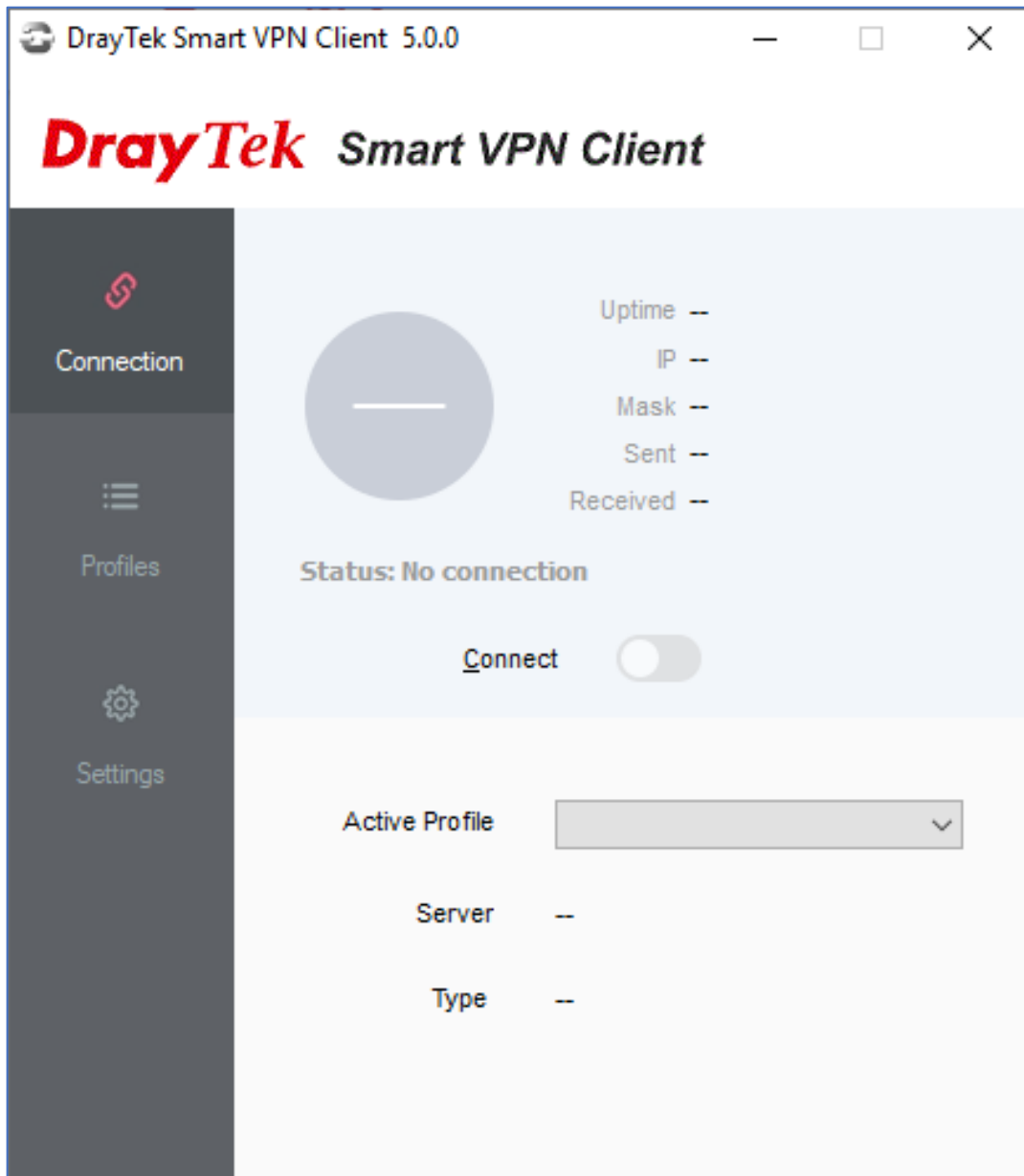
Klik op OK om het VPN profiel op te slaan, u krijgt in het overzichtsscherm te zien welke VPN gebruiker u hebt aangemaakt.

Remote Access User Accounts: [Set to Factory Default](#)

Index	Enable	User	Status	Index	Enable	User	Status
1.	<input checked="" type="checkbox"/>	draytek	LAN1-192.168.1.250	17.	<input type="checkbox"/>	???	---
2.	<input type="checkbox"/>	???	---	18.	<input type="checkbox"/>	???	---

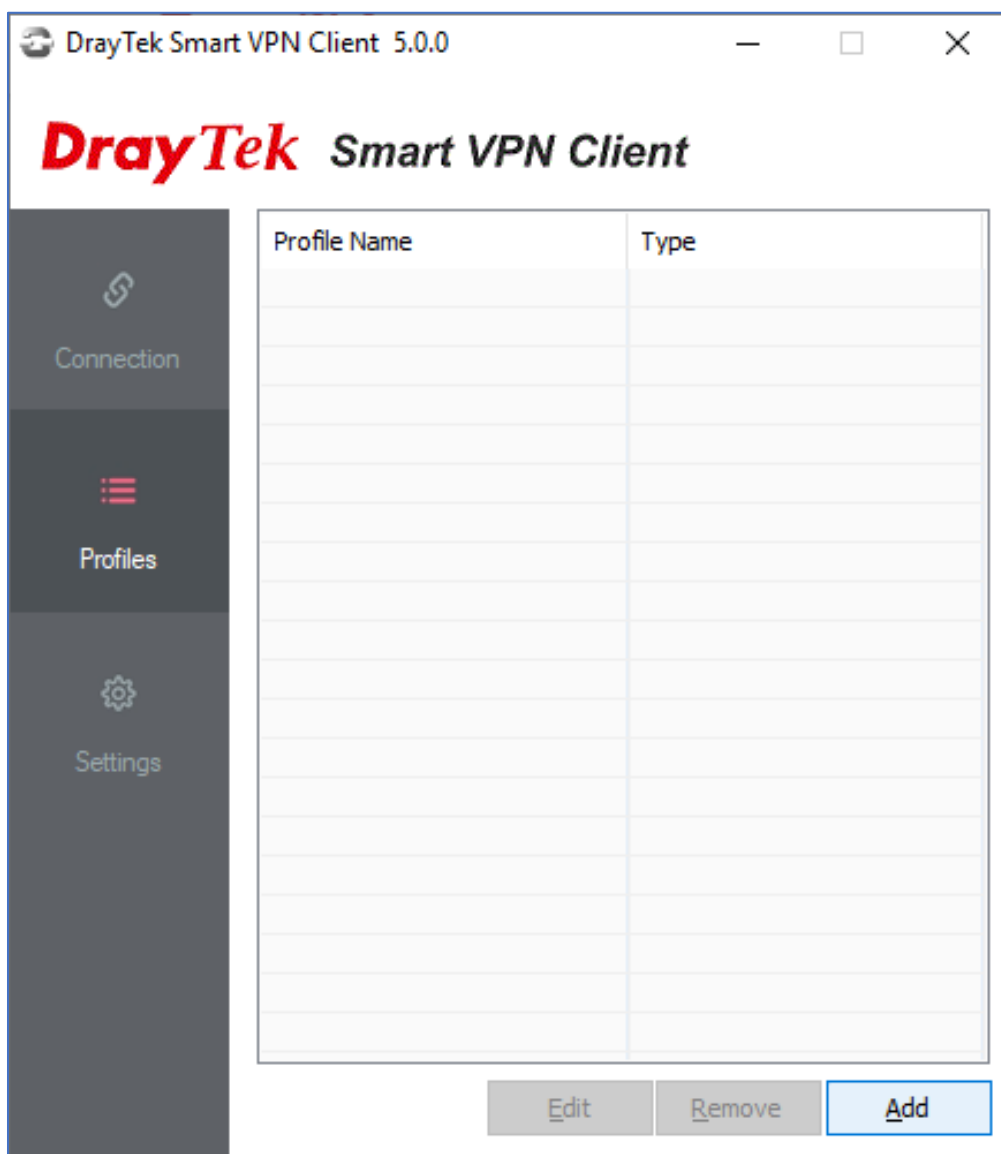
## PPTP VPN verbinding via Smart VPN Client

U dient de Smart VPN Client te installeren, vervolgens kunt u deze openen zodat u onderstaand scherm te zien krijgt.



U hebt aan de linkerkant een 3-tal menu opties, om een VPN aan te kunnen maken gaat u naar Profiles. Klik op Add om een nieuw VPN profiel aan te maken.





De volgende instellingen zijn van belang bij het configureren van een PPTP verbinding:

- VPN Server IP/HOST Name:** Het IP-adres van de VPN server waarnaar u de verbinding wilt opzetten.
- Username & Password:** Gebruikersnaam en wachtwoord van uw VPN profiel, deze moet bekend zijn bij de VPN server.
- Type of VPN:** Selecteer hier PPTP.

Klik op OK om het VPN profiel op te slaan.

Enkele extra mogelijkheden bij het inrichten/opzetten van een VPN profiel:

**IP Property:**

Hier geeft u aan of op basis van DHCP of Static een VPN verbinding moet worden opgezet.

**Advanced Settings:**

Hier kunt u de authenticatie en encryptie methode aanpassen. Deze staat standaard op Auto waardoor de VPN client automatisch bekijkt welke methode gebruikt dient te worden bij de VPN verbinding. Daarnaast kunt u aangeven of u al het verkeer over de VPN tunnel wil sturen. Standaard staat deze optie niet aan zodat internet verkeer gewoon via de lokale internet verbinding zal verlopen. Door dit vinkje in te schakelen zorgt u ervoor dat al het verkeer via de VPN tunnel zal verlopen.

**IP Property** ▼

Automatically get IP address and DNS server  
 Manually set IP address and DNS server

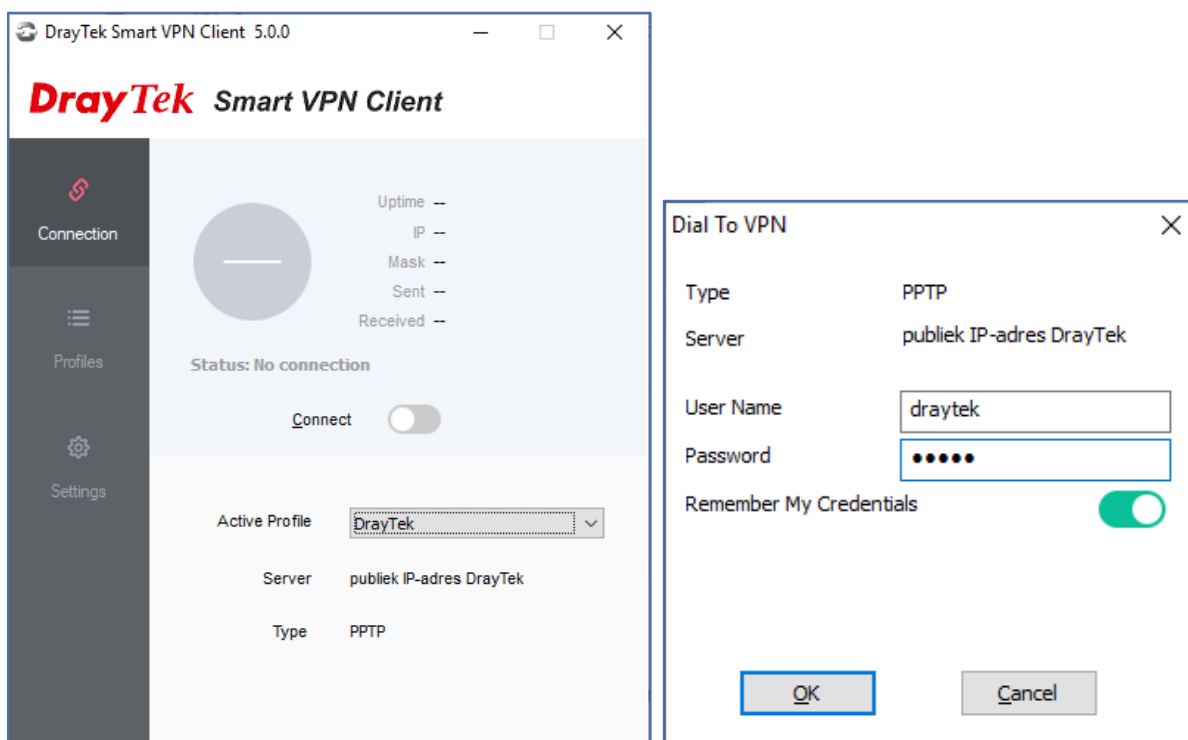
IP address: 192 . 168 . 1 . 10  
DNS address: 192 . 168 . 1 . 1  
WINS Server: . . .

**Advanced Options** ▼

Authentication Method: AUTO ▼  
MPPE Encryption: AUTO ▼  
Enable NetBIOS over TCP/IP:   
Use default gateway on remote network:   
More

Cancel OK

Bij het menu Connection kun je de VPN verbinding opzetten, klik op de connect checkbox.

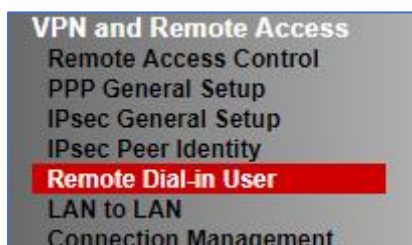


Indien de VPN tunnel online is kunt u middels een simpele ping test achterhalen of de VPN tunnel succesvol werkt.

```
Pingen naar 192.168.1.1 met 32 bytes aan gegevens:  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
  
Ping-statistieken voor 192.168.1.1:  
Pakketten: verzonden = 4, ontvangen = 4, verloren = 0  
(0% verlies).  
  
De gemiddelde tijd voor het uitvoeren van één bewerking in milliseconden:  
Minimum = 5ms, Maximum = 5ms, Gemiddelde = 5ms
```

## DrayTek VPN Remote Dial In configuratie – IPsec VPN

In het menu gaat u naar VPN and Remote Access om vervolgens te klikken op Remote Dial In User.



U komt op een overzichtsscherm terecht waarin nog geen actieve profielen staan. Om een nieuw profiel aan te maken klikt u op het juiste index nummer.

VPN and Remote Access >> Remote Dial-in User ?

Remote Access User Accounts: | [Set to Factory Default](#) |

Index	Enable	User	Status	Index	Enable	User	Status
<a href="#">1.</a>	<input type="checkbox"/>	???	---	<a href="#">17.</a>	<input type="checkbox"/>	???	---
<a href="#">2.</a>	<input type="checkbox"/>	???	---	<a href="#">18.</a>	<input type="checkbox"/>	???	---
<a href="#">3.</a>	<input type="checkbox"/>	???	---	<a href="#">19.</a>	<input type="checkbox"/>	???	---
<a href="#">4.</a>	<input type="checkbox"/>	???	---	<a href="#">20.</a>	<input type="checkbox"/>	???	---
<a href="#">5.</a>	<input type="checkbox"/>	???	---	<a href="#">21.</a>	<input type="checkbox"/>	???	---
<a href="#">6.</a>	<input type="checkbox"/>	???	---	<a href="#">22.</a>	<input type="checkbox"/>	???	---
<a href="#">7.</a>	<input type="checkbox"/>	???	---	<a href="#">23.</a>	<input type="checkbox"/>	???	---

Bij het configureren van een IPsec Remote Dial In profiel zijn onderstaande instellingen van belang:

- Enable this Account:** Door hier een vinkje te zetten activeert u het VPN profiel.
- Allowed Dial In Type:** Selecteer het juiste VPN Protocol wat u wilt gebruiken. In dit geval selecteert u IPsec.
- Specify Remote Node:** Hier geeft u het publieke IP-adres op van de remote client, aan de hand van dit IP-adres voert de DrayTek een beveiligingscontrole uit. Indien dit IP-adres niet bekend is of telkens verschillend kan hierop geen controle plaatsvinden. Specify Remote Node hoeft u dan niet aan te vinken.
- Pre-Shared Key:** Geef hier de juiste Pre-Shared Key op. Dit is alleen mogelijk wanneer het gebruik wordt gemaakt van Specify Remote Node.

Wanneer het Remote Client IP telkens verschillend is, kunt u geen Pre-Shared Key opgeven in het VPN profiel. U kunt er dan voor kiezen om een algemene Pre-Shared Key op te geven bij het IPsec General Setup menu. Deze algemene Pre-Shared Key is geldig voor alle VPN accounts waarvan het Remote Client IP-adres niet bekend is.

**VPN IKE/IPsec General Setup**  
Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

**IKE Authentication Method**  
Certificate for Dial-in:

**General Pre-Shared Key**  
Pre-Shared Key:   
Confirm Pre-Shared Key:

**Pre-Shared Key for XAuth User**  
Pre-Shared Key:   
Confirm Pre-Shared Key:

**IPsec Security Method**  
 Medium (AH)  
Data will be authenticated, but will not be encrypted.

High (ESP)  DES  3DES  AES  
Data will be encrypted and authenticated.

Onderstaande afbeelding geeft een voorbeeld IPsec Remote Dial In profiel weer.

**User account and Authentication**  
 Enable this account  
Idle Timeout:  second(s)

**Allowed Dial-In Type**  
 PPTP  
 IPsec Tunnel  
 L2TP with IPsec Policy:   
 SSL Tunnel  
 IPsec XAuth

Specify Remote Node  
Remote Client IP:   
or Peer ID:   
Netbios Naming Packet:  Pass  Block  
Multicast via VPN:  Pass  Block  
(for some IGMP,IP-Camera,DHCP Relay..etc.)

**Subnet**  
  
 Assign Static IP Address

Username:   
Password:   
 Enable Mobile One-Time Passwords(mOTP)  
PIN Code:   
Secret:

**IKE Authentication Method**  
 Pre-Shared Key  
IKE Pre-Shared Key:   
 Digital Signature(X.509)

**IPsec Security Method**  
 Medium(AH)  
High(ESP)  DES  3DES  AES  
Local ID (optional):

Dit zijn de basis instellingen welke belangrijk zijn voor het opzetten/instellen van een VPN Remote Dial In User op basis van IPsec.

Klik op OK om het VPN profiel op te slaan, u krijgt in het overzichtsscherm te zien welke VPN gebruiker u hebt aangemaakt.

Remote Access User Accounts:				<a href="#">Set to Factory Default</a>			
Index	Enable	User	Status	Index	Enable	User	Status
<u>1.</u>	<input checked="" type="checkbox"/>	draytek	LAN1-192.168.1.250	<u>17.</u>	<input type="checkbox"/>	???	---
<u>2.</u>	<input type="checkbox"/>	???	---	<u>18.</u>	<input type="checkbox"/>	???	---

## IPSec VPN verbinding via Smart VPN Client

De volgende instellingen zijn van belang bij het configureren van een IPSec profiel in de DrayTek Smart VPN Client.

**Profile Name:** naam van het VPN profiel

**Type:** IPSec Tunnel

**IP or Hostname:** Publiek IP-adres van de DrayTek waarmee u een VPN wilt maken

**Edit Profile** [X]

Profile Name

**Server Information**

Type

IP or Hostname

**Login Information**

Authentication Type

User Name

Password

Remember My Credentials

Always Prompt for Credentials

**IP Property ▲**

**Advanced Options ▲**



Klik op OK om de instellingen op te slaan. Ga naar het Connection menu, hier kunt u de VPN tunnel activeren door op de Active checkbox te klikken. Vul de Pre-shared Key in die overeenkomt met de Pre-Shared Key in de DrayTek modem/router.

Dial To VPN

Type IPSec Tunnel

Server 1.1.1.1

My IP 10.0.0.44

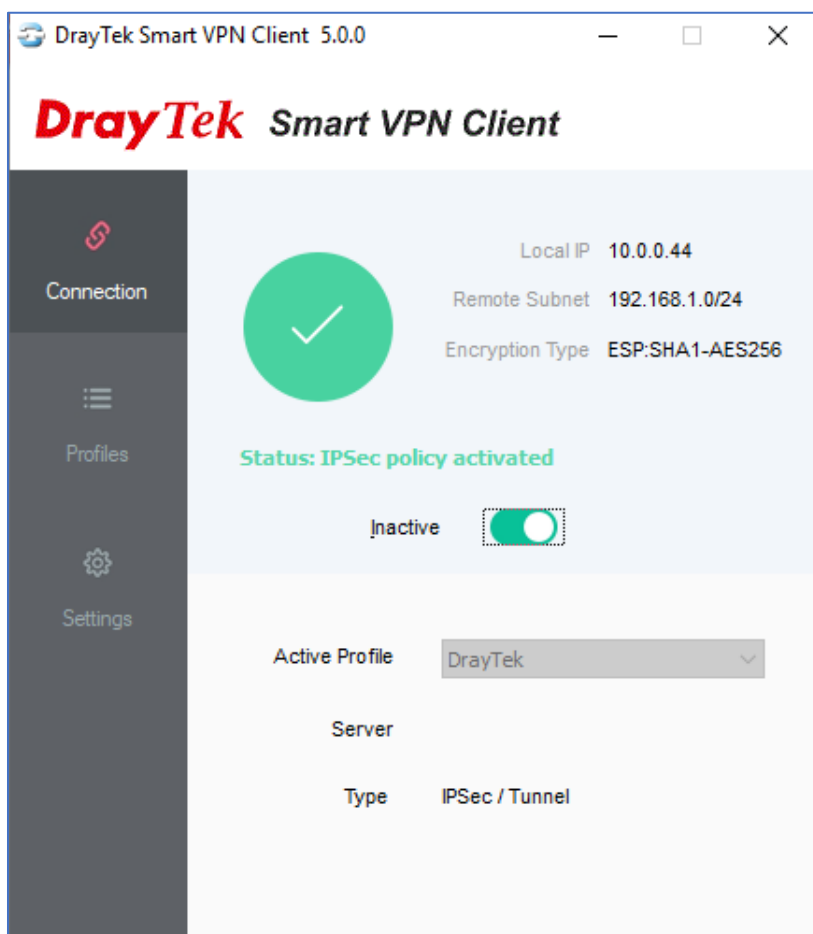
Authentication Method

Pre-shared Key

Certificate Authentication

Browse

OK Cancel

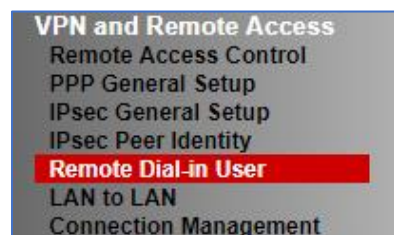


Indien de VPN tunnel online is kunt u middels een simpele ping test achterhalen of de VPN tunnel succesvol werkt.

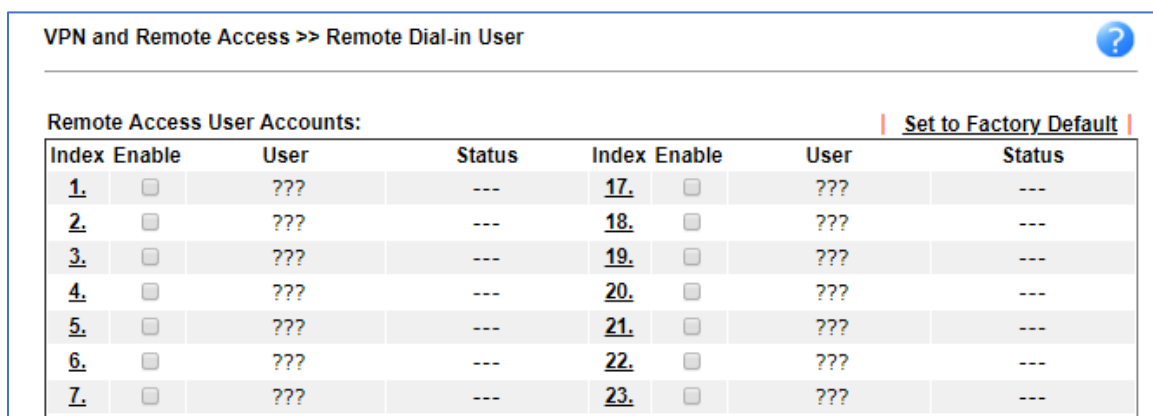
```
Pingen naar 192.168.1.1 met 32 bytes aan gegevens:  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
  
Ping-statistieken voor 192.168.1.1:  
Pakketten: verzonden = 4, ontvangen = 4, verloren = 0  
<0% verlies>.  
  
De gemiddelde tijd voor het uitvoeren van één bewerking in milliseconden:  
Minimum = 5ms, Maximum = 5ms, Gemiddelde = 5ms
```

## DrayTek VPN Remote Dial In configuratie – L2TP over IPsec VPN

Ga naar het menu **VPN and Remote Access**. Kies vervolgens voor Remote Dial-in User.



Het scherm dat nu verschijnt geeft de beschikbare profielen weer. Open een profiel welke nog niet gebruikt wordt. Dit kunt u doen door op het index nummer te klikken, in ons geval klikken we op 1.



The screenshot shows the 'VPN and Remote Access >> Remote Dial-in User' configuration page. It features a table of 'Remote Access User Accounts' with columns for Index, Enable, User, and Status. A 'Set to Factory Default' link is visible on the right. The table contains 14 rows of user accounts, with the first row (Index 1) being the one to be selected.

Remote Access User Accounts:				Set to Factory Default			
Index	Enable	User	Status	Index	Enable	User	Status
<u>1.</u>	<input type="checkbox"/>	???	---	<u>17.</u>	<input type="checkbox"/>	???	---
<u>2.</u>	<input type="checkbox"/>	???	---	<u>18.</u>	<input type="checkbox"/>	???	---
<u>3.</u>	<input type="checkbox"/>	???	---	<u>19.</u>	<input type="checkbox"/>	???	---
<u>4.</u>	<input type="checkbox"/>	???	---	<u>20.</u>	<input type="checkbox"/>	???	---
<u>5.</u>	<input type="checkbox"/>	???	---	<u>21.</u>	<input type="checkbox"/>	???	---
<u>6.</u>	<input type="checkbox"/>	???	---	<u>22.</u>	<input type="checkbox"/>	???	---
<u>7.</u>	<input type="checkbox"/>	???	---	<u>23.</u>	<input type="checkbox"/>	???	---

Bij het configureren van een L2TP over IPsec Remote Dial In profiel zijn onderstaande instellingen van belang:

- Enable this Account:** Door hier een vinkje te zetten activeert u het VPN profiel.
- Allowed Dial In Type:** Selecteer het juiste VPN Protocol wat u wilt gebruiken. In dit geval selecteert u L2TP over IPsec met als Policy Must.
- Specify Remote Node:** Hier geeft u het publieke IP-adres op van de remote client, aan de hand van dit IP-adres voert de DrayTek een beveiligingscontrole uit. Indien dit IP-adres niet bekend is of telkens verschillend is kan hierop geen controle plaatsvinden. Specify Remote Node hoeft u dan niet aan te vinken.
- Pre-Shared Key:** Hier geeft u de juiste Pre-Shared Key op. Dit is alleen mogelijk wanneer het gebruik wordt gemaakt van Specify Remote Node.
- Username & Password:** Geef hier de juiste gebruikersnaam/wachtwoord gegevens op voor het VPN account.

Wanneer het Remote Client IP telkens verschillend is, kunt u zoals hierboven aangegeven geen Pre-Shared Key opgeven in het VPN profiel. U kunt er dan voor kiezen om een algemene Pre-Shared Key op te geven bij het IPsec General Setup menu. Deze algemene Pre-Shared Key is geldig voor alle VPN accounts waarvan het Remote Client IP-adres niet bekend is.

**VPN IKE/IPsec General Setup**  
Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

**IKE Authentication Method**

Certificate for Dial-in

**General Pre-Shared Key**

Pre-Shared Key

Confirm Pre-Shared Key

**Pre-Shared Key for XAuth User**

Pre-Shared Key

Confirm Pre-Shared Key

**IPsec Security Method**

Medium (AH)  
Data will be authenticated, but will not be encrypted.

High (ESP)  DES  3DES  AES  
Data will be encrypted and authenticated.

Onderstaande afbeelding geeft aan hoe het VPN profiel ingesteld zal zijn, dit kunt u natuurlijk naar eigen wens inrichten.

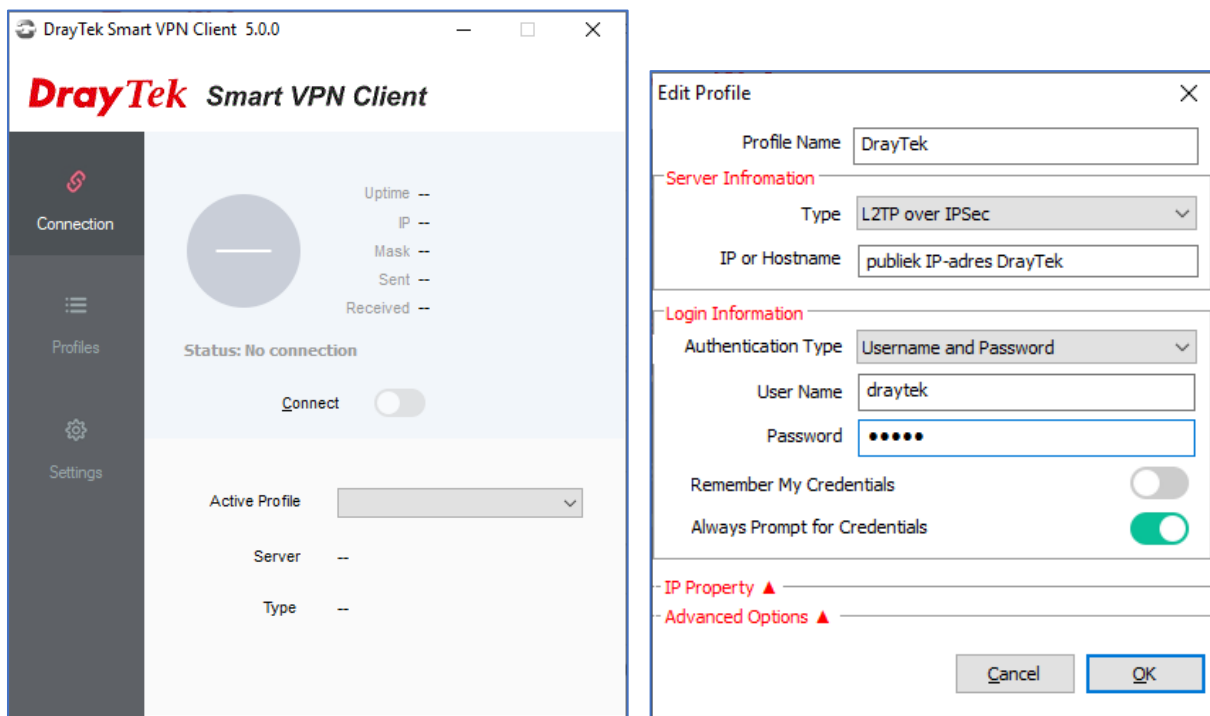
<b>User account and Authentication</b> <input checked="" type="checkbox"/> Enable this account Idle Timeout <input type="text" value="300"/> second(s)		Username <input type="text" value="draytek"/> Password <input type="password" value="....."/> <input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP) PIN <input type="text"/> Code <input type="text"/> Secret <input type="text"/>
<b>Allowed Dial-In Type</b> <input type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="Must"/> <input type="checkbox"/> SSL Tunnel <input type="checkbox"/> IPsec XAuth <input type="checkbox"/> Specify Remote Node Remote Client IP <input type="text"/> or Peer ID <input type="text"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)		<b>IKE Authentication Method</b> <input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="text" value="Max: 64 characters"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/>
<b>Subnet</b> <input type="text" value="LAN 1"/> <input type="checkbox"/> Assign Static IP Address <input type="text" value="0.0.0.0"/>		<b>IPsec Security Method</b> <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID (optional) <input type="text"/>

Dit zijn de basis instellingen welke belangrijk zijn voor het opzetten/instellen van een VPN Remote Dial In User op basis van L2TP over IPsec.

Klik op OK om het VPN profiel op te slaan, u krijgt in het overzichtsscherm te zien welke VPN gebruiker u hebt aangemaakt.

Remote Access User Accounts:								<a href="#">Set to Factory Default</a>
Index	Enable	User	Status	Index	Enable	User	Status	
1.	<input checked="" type="checkbox"/>	draytek	LAN1-192.168.1.250	17.	<input type="checkbox"/>	???	---	
2.	<input type="checkbox"/>	???	---	18.	<input type="checkbox"/>	???	---	

## L2TP over IPsec VPN verbinding via Smart VPN Client

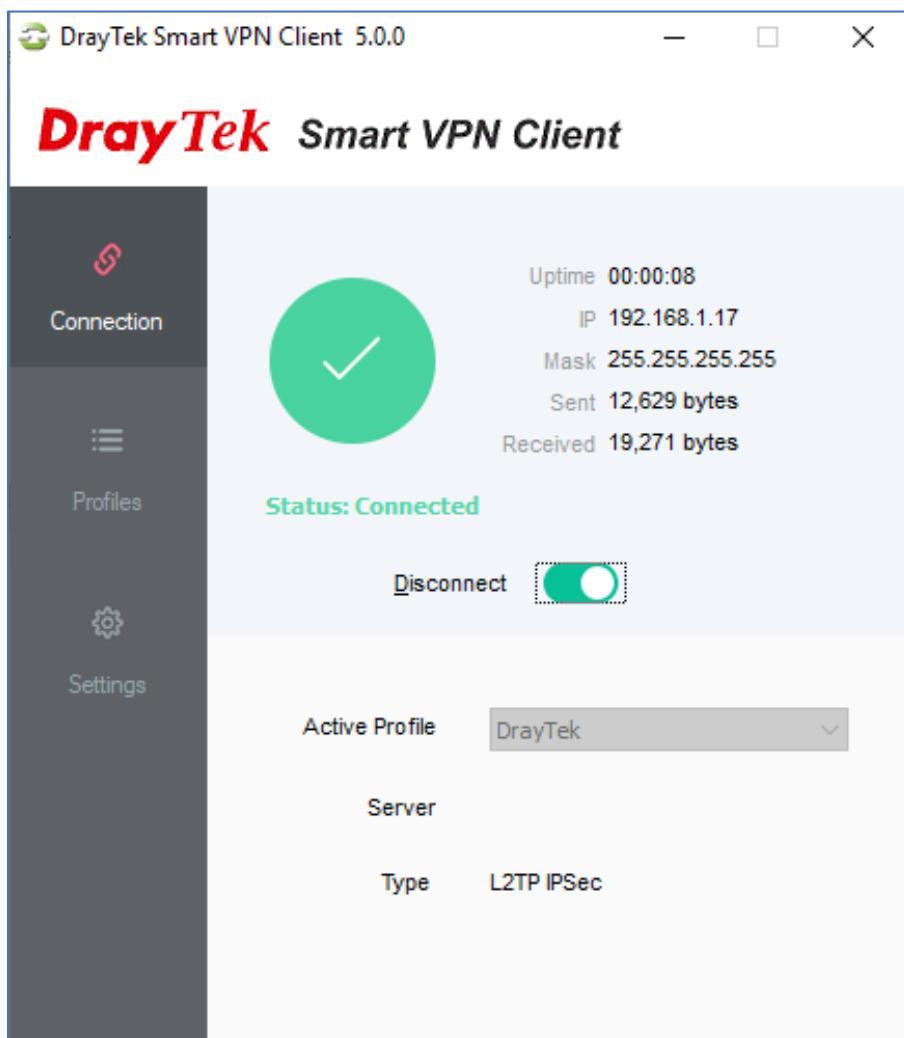


U hebt aan de linkerkant een 3-tal menu opties, om een VPN aan te kunnen maken gaat u naar Profiles. Klik op Add om een nieuw VPN profiel aan te maken.

Bij VPN Server IP/Host geeft u het WAN IP-adres van de DrayTek, hierna wordt de VPN tunnel opgezet. Selecteer daarna L2TP over IPsec Tunnel en klik op OK. De volgende instellingen zijn daarna belangrijk:

<b>Profile Name:</b>	Profiel naam van de VPN verbinding
<b>Type:</b>	L2TP over IPsec
<b>IP or Hostname:</b>	Publiek IP-adres van de DrayTek waarmee u de VPN verbinding wilt maken
<b>Authentication Type:</b>	Username and Password
<b>User Name:</b>	Gebruikersnaam
<b>Password:</b>	Wachtwoord

Klik op OK om de instellingen op te slaan. Ga naar het Connection menu, hier kunt u de VPN tunnel activeren door op de Active checkbox te klikken. Vul de Pre-shared Key in die overeenkomt met de Pre-Shared Key in de DrayTek modem/router.



Indien de VPN tunnel online is kunt u middels een simpele ping test achterhalen of de VPN tunnel succesvol werkt.

```
Pingen naar 192.168.1.1 met 32 bytes aan gegevens:  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
  
Ping-statistieken voor 192.168.1.1:  
Pakketten: verzonden = 4, ontvangen = 4, verloren = 0  
<0% verlies>.  
  
De gemiddelde tijd voor het uitvoeren van één bewerking in milliseconden:  
Minimum = 5ms, Maximum = 5ms, Gemiddelde = 5ms
```

## DrayTek VPN Remote Dial In configuratie – SSL VPN

SSL VPN maakt standaard gebruik van poort 443 (HTTPS), u hebt in de DrayTek de mogelijkheid om deze SSL VPN poort aan te passen. Dit kan bij SSL VPN >> General Setup. Daarnaast kunt u SSL VPN in of uit schakelen per WAN poort.

SSL VPN >> General Setup

---

SSL VPN General Setup

Bind to WAN	<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> WAN2	<input checked="" type="checkbox"/> WAN3	<input checked="" type="checkbox"/> WAN4
Port	<input type="text" value="443"/> (Default: 443)			
Server Certificate	<input type="text" value="self-signed"/> ▼			

Note:

1. The settings will act on all SSL applications.
2. Please go to [System Maintenance >> Management](#) to enable SSLv3.0 .
3. Please go to [System Maintenance >> Self-Signed Certificate](#) to generate a new "self-signed" certificate.

In het VPN menu gaat u daarna naar VPN and Remote Access om vervolgens te klikken op Remote Dial In User.



U komt op een overzichtsscherm terecht waarin nog geen actieve profielen staan. Door een nieuw profiel aan te maken klikt u op het juiste index nummer.

VPN and Remote Access >> Remote Dial-in User ?

---

Remote Access User Accounts: | [Set to Factory Default](#) |

Index	Enable	User	Status	Index	Enable	User	Status
<u>1.</u>	<input type="checkbox"/>	???	---	<u>17.</u>	<input type="checkbox"/>	???	---
<u>2.</u>	<input type="checkbox"/>	???	---	<u>18.</u>	<input type="checkbox"/>	???	---
<u>3.</u>	<input type="checkbox"/>	???	---	<u>19.</u>	<input type="checkbox"/>	???	---
<u>4.</u>	<input type="checkbox"/>	???	---	<u>20.</u>	<input type="checkbox"/>	???	---
<u>5.</u>	<input type="checkbox"/>	???	---	<u>21.</u>	<input type="checkbox"/>	???	---
<u>6.</u>	<input type="checkbox"/>	???	---	<u>22.</u>	<input type="checkbox"/>	???	---
<u>7.</u>	<input type="checkbox"/>	???	---	<u>23.</u>	<input type="checkbox"/>	???	---



Bij het configureren van een SSL Remote Dial In profiel zijn onderstaande instellingen van belang:

- Enable this Account:** Door hier een vinkje te zetten activeert u het VPN profiel.
- Idle Timeout:** Deze optie staat standaard op 300 seconden, dit betekent dat de DrayTek de VPN verbinding zal verbreken indien er 5 minuten geen activiteit plaatsvindt. U kunt deze optie eventueel op 0 seconden zetten, zodoende zal de DrayTek hierop geen controle meer uitvoeren.
- Allowed Dial In Type:** Selecteer het juiste VPN Protocol wat u wilt gebruiken. In dit geval selecteert u SSL Tunnel.
- Specify Remote Node:** Hier geeft u het publieke IP-adres op van de remote client, aan de hand van dit IP-adres voert de DrayTek een beveiligingscontrole uit. Indien dit IP-adres niet bekend is of telkens verschillend is hoeft u deze instelling niet op te geven. In dat geval hoeft u deze optie niet in te schakelen.
- Username/Password:** Geef hier de juiste gebruikersnaam/wachtwoord gegevens op voor het VPN account.
- Subnet:** Indien u gebruik maakt van meerdere LAN subnetten kunt u hier aangeven in welk LAN subnet deze VPN gebruiker moet komen wanneer een verbinding wordt opgezet.

Op de volgende pagina staat een afbeelding welke een voorbeeld configuratie aangeeft, deze kunt u natuurlijk naar uw eigen wens inrichten.

<b>User account and Authentication</b> <input checked="" type="checkbox"/> Enable this account Idle Timeout <input type="text" value="300"/> second(s)		Username <input type="text" value="draytek"/> Password <input type="password" value="....."/> <input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP) PIN Code <input type="text"/> Secret <input type="text"/>
<b>Allowed Dial-In Type</b> <input type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/> <input checked="" type="checkbox"/> SSL Tunnel <input type="checkbox"/> IPsec XAuth <input type="checkbox"/> Specify Remote Node Remote Client IP <input type="text"/> or Peer ID <input type="text"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)		<b>IKE Authentication Method</b> <input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="text" value="Max: 64 characters"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/>
<b>Subnet</b> <input type="text" value="LAN 1"/> <input type="checkbox"/> Assign Static IP Address <input type="text" value="0.0.0.0"/>		<b>IPsec Security Method</b> <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID (optional) <input type="text"/>

Dit zijn de basis instellingen welke belangrijk zijn voor het opzetten/instellen van een VPN Remote Dial In User op basis van SSL. Nu kunt u er bijvoorbeeld ook voor kiezen om elke VPN gebruiker een vast IP-adres te geven. Dit kunt u doen door een vinkje te zetten bij Assign Static IP Address.

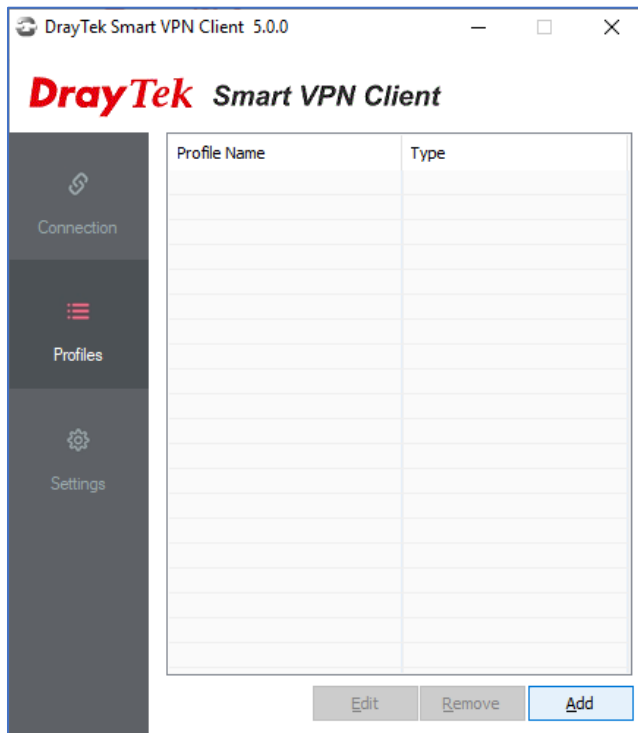
<b>Subnet</b> <input type="text" value="LAN 1"/> <input checked="" type="checkbox"/> Assign Static IP Address <input type="text" value="192.168.1.250"/>
---

Klik op OK om het VPN profiel op te slaan, u krijgt in het overzichtsscherm te zien welke VPN gebruiker u hebt aangemaakt.

Remote Access User Accounts:				<a href="#">Set to Factory Default</a>			
Index	Enable	User	Status	Index	Enable	User	Status
1.	<input checked="" type="checkbox"/>	draytek	LAN1-192.168.1.250	17.	<input type="checkbox"/>	???	---
2.	<input type="checkbox"/>	???	---	18.	<input type="checkbox"/>	???	---

## SSL VPN verbinding via Smart VPN Client

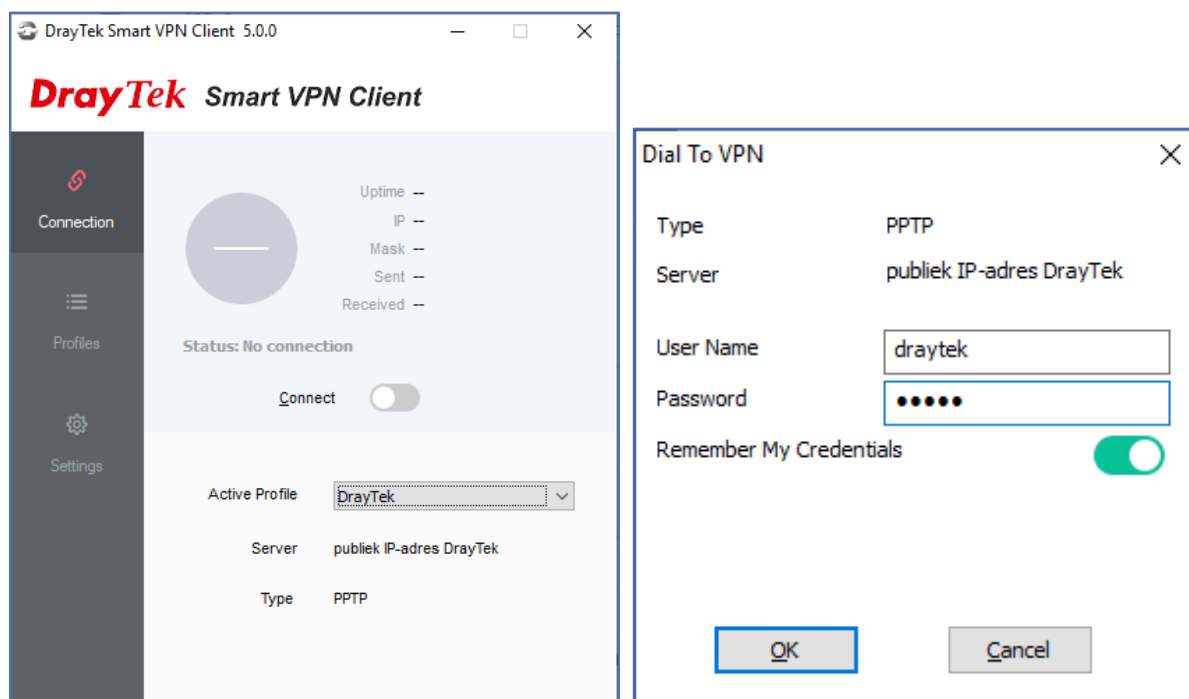
U hebt aan de linkerkant een 3-tal menu opties, om een VPN aan te kunnen maken gaat u naar Profiles. Klik op Add om een nieuw VPN profiel aan te maken.



De volgende instellingen zijn van belang bij het configureren van een SSL verbinding:

- Profile Name:** Profiel naam van de VPN tunnel
- Type:** SSL VPN Tunnel
- IP or Hostname:** Publiek IP-adres van de DrayTek waarmee u de VPN verbinding wilt maken
- Authentication Type:** Username and Password
- User Name:** gebruikersnaam
- Password:** wachtwoord

Bij het menu Connection kun je de VPN verbinding opzetten, klik op de connect checkbox.



Indien de VPN tunnel online is kunt u middels een simpele ping test achterhalen of de VPN tunnel succesvol werkt.

```
Pingen naar 192.168.1.1 met 32 bytes aan gegevens:  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
Antwoord van 192.168.1.1: bytes=32 tijd=5 ms TTL=251  
  
Ping-statistieken voor 192.168.1.1:  
Pakketten: verzonden = 4, ontvangen = 4, verloren = 0  
(0% verlies).  
  
De gemiddelde tijd voor het uitvoeren van één bewerking in milliseconden:  
Minimum = 5ms, Maximum = 5ms, Gemiddelde = 5ms
```

### **Voorbehoud**

We behouden ons het recht voor om deze en andere documentatie te wijzigen zonder de verplichting gebruikers hiervan op de hoogte te stellen. Afbeeldingen en screenshots kunnen afwijken.

### **Copyright verklaring**

© 2020 DrayTek

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder voorafgaande schriftelijke toestemming van de uitgever.

Ondanks alle aan de samenstelling van deze handleiding bestede zorg kan noch de fabrikant, noch de auteur, noch de distributeur aansprakelijkheid aanvaarden voor schade die het gevolg is van enige fout uit deze uitgave.

### **Trademarks**

Alle merken en geregistreerde merken zijn eigendom van hun respectievelijke eigenaren.