

DrayTek

DrayOS 4
EasyVPN



Inhoudsopgave

EasyVPN	3
Router en software ondersteuning	4
Model / Applicatie ondersteuning	4
VPN protocolondersteuning per OS	4
DrayDDNS met Let's Encrypt certificaat.....	4
Vigor router configuratie	5
VPN diensten inschakelen en configureren.....	5
WireGuard configuratie.....	6
OpenVPN configuratie.....	6
IPsec configuratie.....	7
Remote Dial In user configuratie	8
Windows Smart VPN Client.....	10
Android SmartVPN App.....	12
iOS Smart VPN App.....	13
macOS Smart VPN App	14

EasyVPN

De Vigor Router ondersteunt verschillende VPN-protocollen, zoals IPsec, WireGuard en OpenVPN. Door het brede aanbod van protocollen en configuraties kunnen gebruikers echter moeilijkheden ondervinden bij het kiezen van het juiste protocol, het instellen ervan of het tot stand brengen van een VPN-verbinding door externe omgevingsfactoren. Om deze problemen te verminderen, heeft DrayTek een nieuwe EasyVPN functie ontwikkeld.

Met EasyVPN hoeven gebruikers geen WireGuard-sleutels meer te genereren, OpenVPN bestanden te importeren of certificaten te uploaden. Het opzetten van een VPN-verbinding kan eenvoudig door alleen een gebruikersnaam en wachtwoord in te vullen of een eenmalige code (OTP) per e-mail te ontvangen.

Als een VPN verbinding om welke reden dan ook niet tot stand kan worden gebracht, schakelt de EasyVPN client automatisch over naar het volgende beschikbare VPN protocol en probeert opnieuw verbinding te maken.

Introductie video: <https://www.youtube.com/watch?v=wOYUWzDCfxk>



Router en software ondersteuning

Zorg er voor dat zowel de router firmware als de Smart VPN software beschikken over de meest recente versies. Deze zijn beschikbaar op www.draytek.nl/support.

Model / Applicatie ondersteuning

Model / Applicatie	Versie
Vigor2136, C410, C510 serie	Firmware 5.3.1(zie DrayOS 5 handleiding)
Vigor2962, 3910, 3912 serie	Firmware 4.4.5
Windows Smart VPN Client	v5.7.1
Android Smart VPN App	v1.6.0
iOS Smart VPN App	v1.9.6
macOS Smart VPN App	v1.8.0
Linux EasyVPN Client	v1.0.0

VPN protocolondersteuning per OS

VPN Type	Windows	iOS	macOS	Android	Linux
IPsec IKEv1 PSK	Y				Y
IPsec IKEv1 XAuth		Y	Y		
IPsec IKEv2 PSK					Y
IPsec IKEv2 EAP	Y	Y	Y		Y
WireGuard	Y			Y	Y
OpenVPN	Y			Y	Y

DrayDDNS met Let's Encrypt certificaat

DrayTek biedt voor elke Vigor-router een volledig gratis DDNS-dienst aan: DrayDDNS. Met DrayDDNS kunt u een gratis hostnaam kiezen binnen het domein drayddns.com, inclusief een gratis SSL-certificaat van Let's Encrypt om uw domeinnaam te beveiligen.

Sommige besturingssystemen vereisen deze extra beveiliging om een VPN-verbinding tot stand te kunnen brengen. Bovendien is een hostnaam makkelijker te onthouden en altijd bruikbaar, zelfs wanneer het IP-adres van uw internetprovider verandert.

Voor het aanmaken van DrayDDNS en activeren van Let's Encrypt, kunt u de volgende handleiding op onze website raadplegen: [Dynamic DNS - DrayDDNS](#)

Vigor router configuratie

VPN diensten inschakelen en configureren

Navigeer in de WebUI van de DrayTek naar “**VPN and Remote Access > Remote Access Control**” en schakel alle VPN-diensten in en configureer de bijbehorende instellingen. Na inschakelen is het noodzakelijk de DrayTek te herstarten.

VPN and Remote Access >> Remote Access Control

Remote Access Control Setup	Bind to WAN
☐ Enable PPTP VPN Service	☐ Port Knocking None ▾
☒ Enable IPsec VPN Service	☐ Port Knocking None ▾
☐ Enable L2TP VPN Service	☐ Port Knocking None ▾
☒ Enable EasyVPN / SSL VPN Service	☐ Port Knocking Follow HTTPS ▾ ?
☒ Enable OpenVPN Service	☐ Port Knocking None ▾
☒ Enable WireGuard VPN Service	☐ Port Knocking None ▾

Note:

1. To allow VPN pass-through to a separate VPN server on the LAN, disable the services listed above that use the same protocol and ensure that NAT Open Ports or Port Redirection is well-configured.
2. Disable unused VPN services, enable Brute Force Protection, and block unknown IP access to the used VPN services to reduce Cyberattacks.
3. Enable Port Knocking to protect VPN services from malicious access attempts over the Internet. All VPN services will use the same Port Knocking profile, allowing the VPN client to connect using different VPN protocols as needed.

EasyVPN / SSL VPN:

Indien de port op 443 staat dient HTTPS toegang vanaf de WAN ingeschakeld zijn (zonder access list) om de EasyVPN gebruikers te laten communiceren met de EasyVPN-server.

- **Port:** Met deze optie kunnen gebruikers handmatig de poort voor de EasyVPN configureren. Deze optie geeft tevens onze voorkeur te gebruiken.

VPN and Remote Access >> EasyVPN / SSL Setup

EasyVPN / SSL Setup

Bind to WAN ☒ WAN1 ☒ WAN2

Port (Default: 443)

Server Certificate Default Certificate

EasyVPN Type Preference:

☒ WireGuard

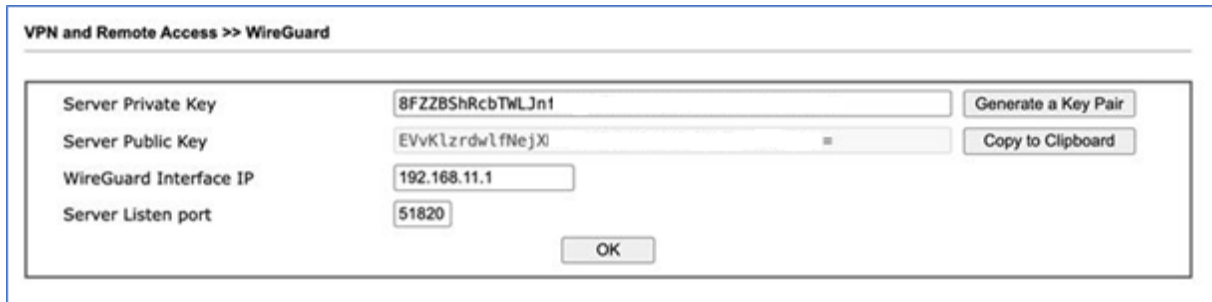
☐ IPsec

☐ OpenVPN

VPN Type Preference: Stelt gebruikers in staat om de prioriteit van inkomende VPN-verbindingen aan te passen. Standaard is de volgorde gebaseerd op VPN-prestaties. Om de volgorde aan te passen, kunt u eenvoudig de items verslepen en herschikken in de gewenste volgorde.

WireGuard configuratie

Genereer bij WireGuard een Server Private en Server Public Key. U hoeft hier verder niets mee te doen. Let op: houd de private key altijd privé en deel deze met niemand!



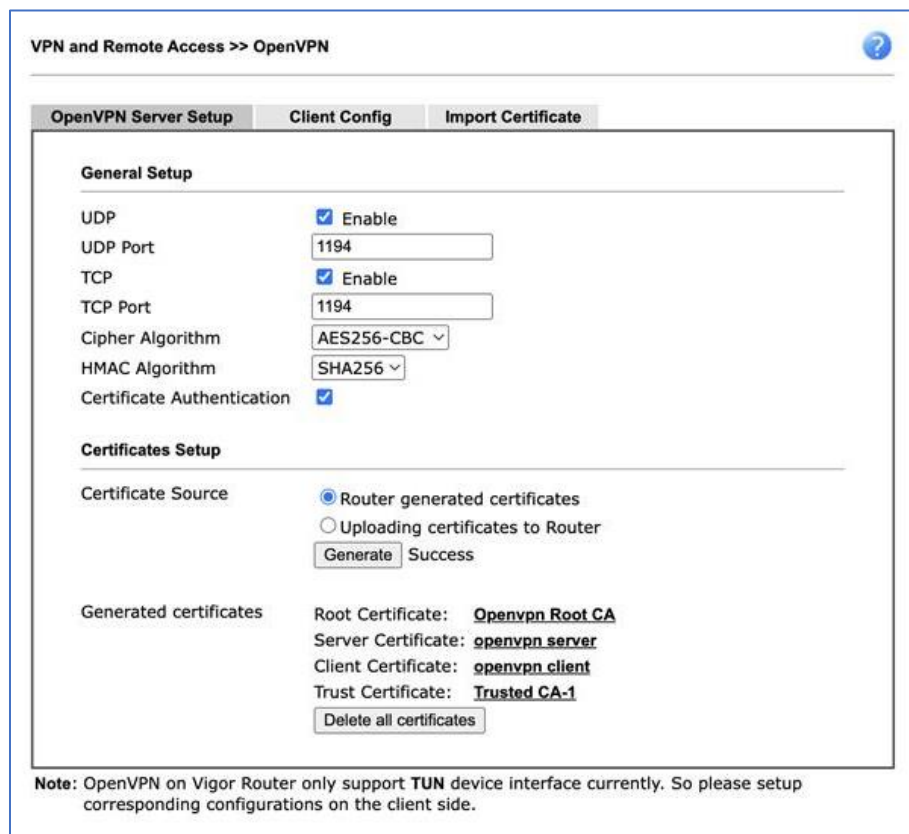
VPN and Remote Access >> WireGuard

Server Private Key	8FZZBShRcbTWLJn1	Generate a Key Pair
Server Public Key	EVvKlZrdwlfNejXl	Copy to Clipboard
WireGuard Interface IP	192.168.11.1	
Server Listen port	51820	

OK

OpenVPN configuratie

Voor OpenVPN dient u eenmalig de certificaten te genereren. U kunt dit proces automatisch door de router laten uitvoeren. Het genereren van de certificaten duurt ongeveer 30 seconden.



VPN and Remote Access >> OpenVPN

OpenVPN Server Setup | Client Config | Import Certificate

General Setup

UDP	☒ Enable
UDP Port	1194
TCP	☒ Enable
TCP Port	1194
Cipher Algorithm	AES256-CBC
HMAC Algorithm	SHA256
Certificate Authentication	☒

Certificates Setup

Certificate Source: ☒ Router generated certificates
☐ Uploading certificates to Router

Generate Success

Generated certificates:

- Root Certificate: [Openvpn Root CA](#)
- Server Certificate: [openvpn server](#)
- Client Certificate: [openvpn client](#)
- Trust Certificate: [Trusted CA-1](#)

Delete all certificates

Note: OpenVPN on Vigor Router only support TUN device interface currently. So please setup corresponding configurations on the client side.

IPsec configuratie

Voor IPsec is het advies gebruik te maken van IKEv2 EAP. Om dit correct in te stellen, dient u de DrayDDNS- en Let's Encrypt-handleiding te volgen. De link naar deze handleiding vindt u op pagina 4.

Ga vervolgens naar IPsec General Setup en selecteer het certificaat dat u hebt aangemaakt binnen het DrayDDNS-profiel. Vul daarnaast een algemene Pre-Shared Key en XAuth User Pre-Shared Key in.

Klik op OK om de instellingen op te slaan.

VPN and Remote Access >> IPsec General Setup

VPN IKE/IPsec General Setup
(Dial-in settings for Remote Dial-In users and LAN-to-LAN VPN Client with Dynamic IP.)

IKE Authentication Method

Version

IKEv1/IKEv2 ▾

Certificate

DrayDDNS (Global) ▾

Preferred Local ID

Alternative Subject Name ▾

General Pre-Shared Key

.....

Confirm General Pre-Shared Key

.....

XAuth User Pre-Shared Key

.....

Confirm XAuth User Pre-Shared Key

.....

IPsec Security Method

☒ Basic ☐ Medium ☐ High

Encryption: AES/3DES/DES
HMAC: SHA256/SHA1/MD5
DH Group: G21/G20/G19/G14/G5/G2/G1
AH: ☒ Enable

VPN TCP maximum segment size (MSS)

IPsec (IKEv1/IKEv2)

1360

(512~1381)

L2TP over IPsec

1360

(512~1361)

GRE over IPsec

1360

(512~1365)

Remote Dial In user configuratie

Bij "Remote Dial-In User" kunt u VPN-profielen aanmaken die verbinding mogen maken via EasyVPN. In onderstaand voorbeeld maken we een VPN-profiel aan dat gebruik mag maken van IPsec, WireGuard en OpenVPN.

Let op: als u gebruik wilt maken van WireGuard, moet u een statisch IP-adres opgeven in het profiel. De WireGuard Peer Setting dient u als laatste te configureren. Dit doet u door op Client Config Generator te klikken.

Belangrijk: voer deze stap pas uit nadat u het statische IP-adres hebt opgegeven.

Index No. 1
☒ Enable this Account
☐ Multiple Concurrent Connections Allowed
Idle Timeout second(s)

Allowed Dial-In Type
☐ PPTP
☒ IPsec Tunnel
☒ IKEv1/IKEv2 ☒ IKEv2 EAP ☒ IPsec XAuth
☐ L2TP with IPsec Policy
☐ SSL Tunnel
☒ OpenVPN Tunnel
☒ WireGuard
☐ Specify Remote Node
Remote Client ☒ IP ☐ Domain Name

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
Two-Factor Authentication
☐ Authentication Code via Email
☐ Authentication Code via SMS
☐ Time-based One-time Password (TOTP)
Secret

User Account and Authentication
Username
Password
☐ Enable Mobile One-Time Passwords(mOTP)
☐ Enable Time-based One-time Password(TOTP)

IKE Authentication Method
☒ Pre-Shared Key

☐ Digital Signature(X.509)

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

WireGuard Peer Setting
Public key
Pre-shared key
Persistent keepalive second(s)

Schedule Profile
 , , ,

Notification
☐ Send Email when VPN is up
Email Object
Mail to
☐ Send SMS when VPN is up
SMS Object
SMS to

WireGuard Peer configuratie

De WireGuard Peer-configuratie hoeft slechts één keer te worden ingesteld. Het is niet noodzakelijk om het gegenereerde WireGuard-configuratiebestand te downloaden.

De belangrijkste instellingen zijn als volgt:

Client Private & Public Key	: Klik op Generate a key pair om een client private en public key te genereren.
Pre-Shared Key	: Klik op Generate om een pre-shared key (PSK) te genereren.
Client IP Address	: Dit veld is reeds ingevuld.
VPN Server	: Vul hier het WAN IP-adres of de DNS-hostnaam in van de router waarmee u de EasyVPN-verbinding wilt opzetten.

Klik vervolgens op Apply to Profile & Close en sla het Remote Dial-In-profiel op door op OK te klikken.

WireGuard Peer configuration Generator

Client Private Key	YJneziXRhKfk8uGJ9	Generate a key pair
Client Public Key	fMIImhuW+xHj1pDZrc	
Pre-Shared Key	MHsZd7zP5T1jvD2w:	Generate
Client IP Address	192.168.11.112	
Persistent Keepalive	60 Seconds	
MTU	1400	
VPN Server	wan.ip.of.hostname	
Set VPN as Default Gateway	☐	
DNS	8.8.8.8, 8.8.4.4	

```
[Interface]
PrivateKey = YJneziXRhKfk8uGJ9
Address = 192.168.11.112/32
DNS = 8.8.8.8, 8.8.4.4
MTU = 1400

[Peer]
PublicKey = EVvK1zrdwlfNejXRY1
PresharedKey = MHsZd7zP5T1jvD2w
AllowedIPs = 192.168.11.0/24
Endpoint = wan.ip.of.hostname :51820
PersistentKeepalive = 60
```

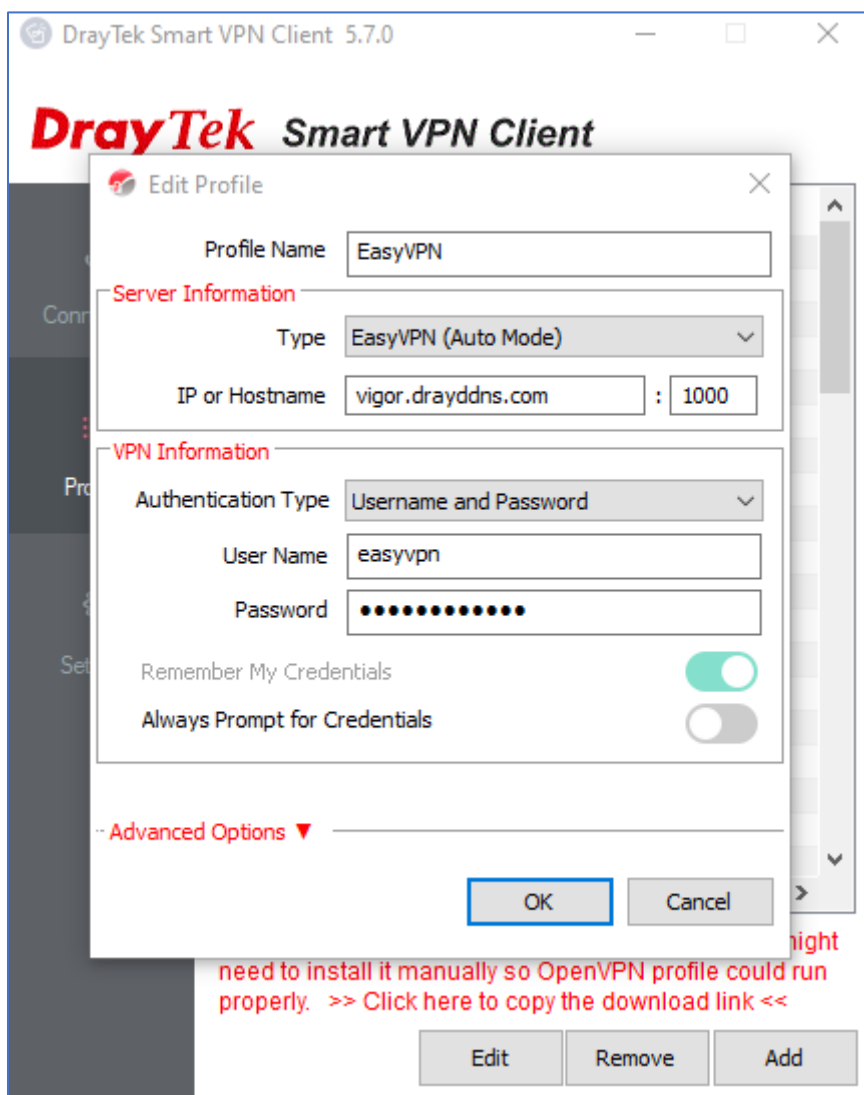


Windows Smart VPN Client

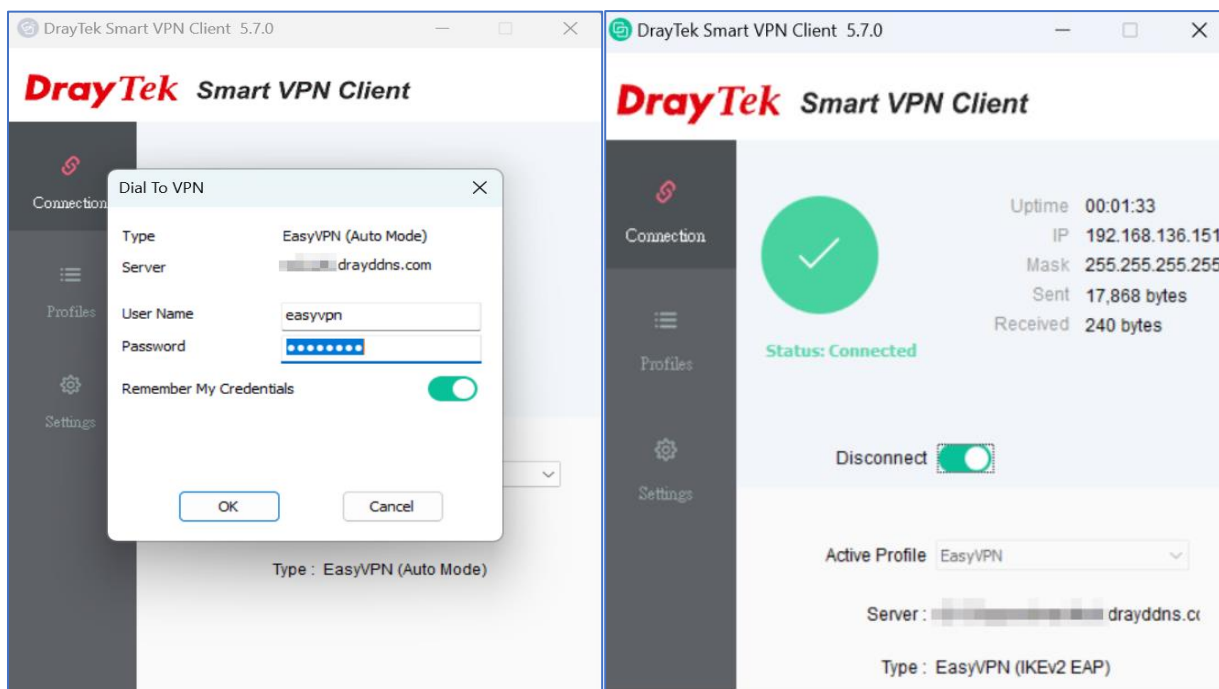
Download en installeer de meest recente Smart VPN Client op www.draytek.nl/support

Open de Smart VPN Client en klik op **Add** om een nieuw profiel aan te maken.
Vul vervolgens de onderstaande gegevens in op basis van uw eerder aangemaakte VPN profiel.

- Profile Name:** Naam van het VPN profiel.
Type: Selecteer EasyVPN (Auto Mode).
IP or Hostname: Vul het IP-adres of domeinnaam in en de EasyVPN poort.
Username: Gebruikersnaam VPN gebruiker.
Password: Wachtwoord VPN gebruiker.

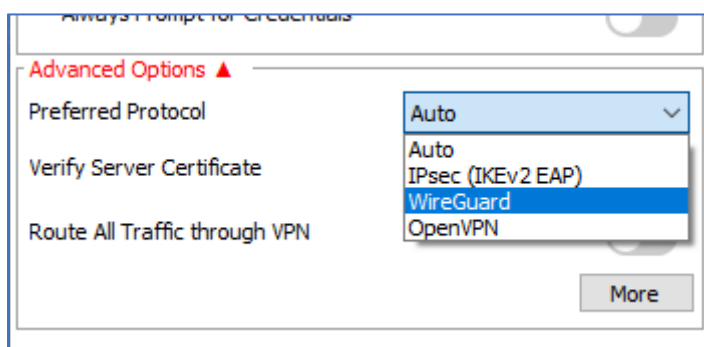


Selecteer het profiel en klik op **Connect**. Vul de gegevens in en klik dan op **OK** om te verbinden.



De EasyVPN verbinding is succesvol tot stand gebracht.

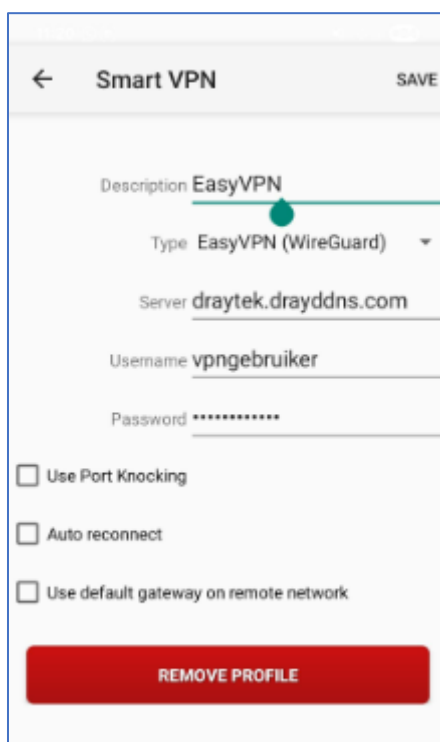
Optioneel: De VPN client bevat een optie voor een voorkeursprotocol, waarmee gebruikers hun gewenste VPN-type kunnen opgeven. Als een gebruiker bijvoorbeeld geen verbinding kan maken via IPsec VPN, maar wel via WireGuard VPN, raden we aan om WireGuard als voorkeursprotocol te selecteren in het VPN-profiel binnen de Smart VPN Client. Hierdoor krijgt WireGuard bij toekomstige verbindingsoogingen voorrang.



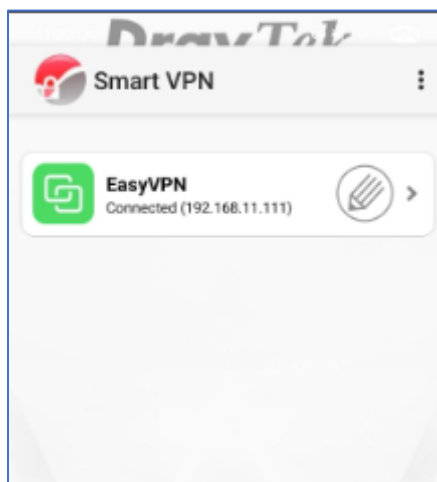
Android SmartVPN App

Download en installeer de SmartVPN App uit de playstore. Open de SmartVPN App en vul de volgende gegevens in:

- Vul een naam in bij Description.
- Selecteer Type: EasyVPN (WireGuard of OpenVPN).
- Vul het IP-adres of de domeinnaam van de VPN-server in, gevolgd door een dubbele punt (:) als EasyVPN-server een aangepaste poort gebruikt.
- Vul de gebruikersnaam en het wachtwoord in.
- Klik op Save om de instellingen op te slaan.



Selecteer het aangemaakte profiel om de VPN verbinding te starten.



iOS Smart VPN App

Download en installeer de SmartVPN App uit de App Store. Open de SmartVPN App en maak een nieuw profiel met de volgende gegevens:

- **Selecteer Type: EasyVPN (Auto Mode).**
- **Voer een naam in bij Profile.**
- **Vul het IP-adres of de domeinnaam van de VPN-server in.**
- **Vul de gebruikte EasyVPN poort in**
- **Voer de gebruikersnaam en het wachtwoord in.**

Type	EasyVPN (Auto Mode) >
Profile	EasyVPN
Server	draytek.drayddns.com
Port	1000
Username	vpngebruiker
Password	
Get Login Code via Email	☐
Enable Port Knocking	☐

Klik op **Save** om de instellingen op te slaan.

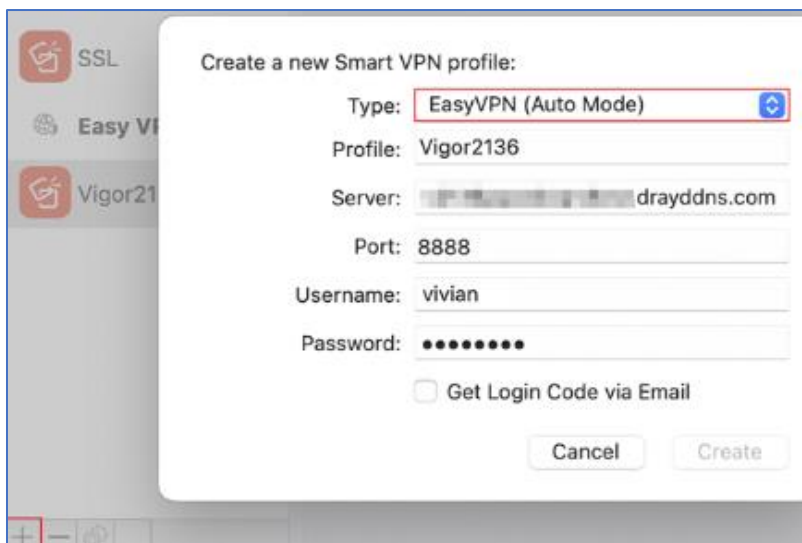
Schakel het profiel in en zet vervolgens het vinkje achter Status aan om de VPN-verbinding te starten. De EasyVPN verbinding is succesvol tot stand gebracht.

Enabled	☒
Status	Connected ☒
Connection Time	0:00:02
Assigned IP	192.168.100.9

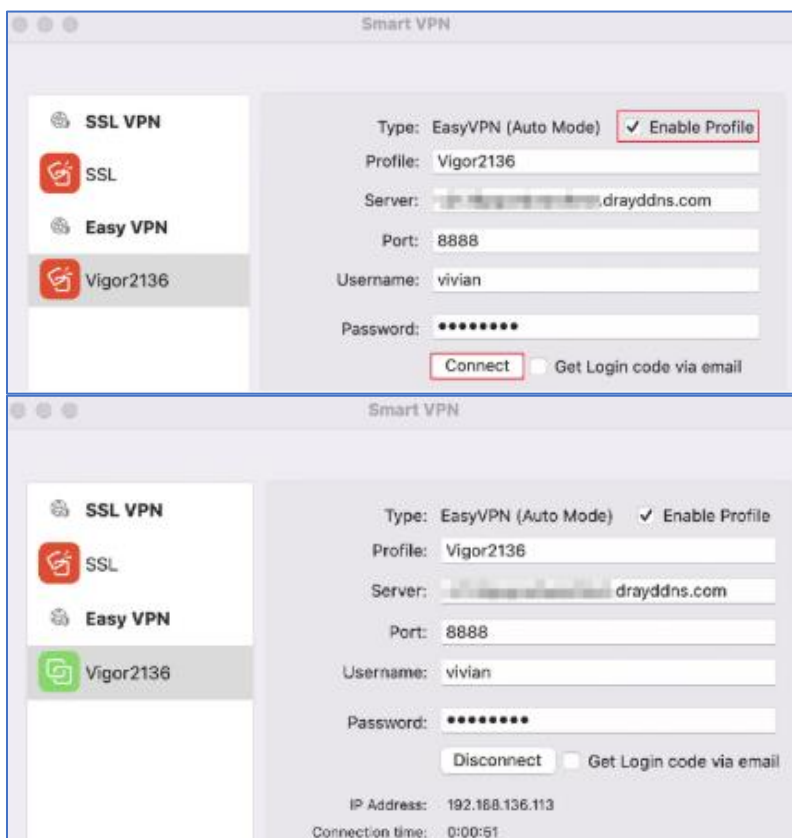
macOS Smart VPN App

Download en installeer de SmartVPN App uit de App Store. Open de SmartVPN App en maak een nieuw profiel met de volgende gegevens:

- **Selecteer Type: EasyVPN (Auto Mode).**
- **Voer een naam in bij Profile.**
- **Vul het IP-adres of de domeinnaam van de VPN-server in.**
- **Vul de gebruikte EasyVPN poort in**
- **Voer de gebruikersnaam en het wachtwoord in.**
- **Klik op Create.**



Selecteer **Enable Profile** en klik op **Connect** om de VPN te starten.





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

© 2025 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.