

***DrayTek***

***VPN***

***IPsec XAuth macOS***



## IPsec XAuth

IPsec XAuth maakt het mogelijk om voor elke gebruiker een eigen VPN account aan te maken, waardoor ze zowel gebruik maken van één algemene XAuth Pre-Shared Key als een gebruikersnaam en wachtwoord. In onderstaande FAQ beschrijven wij de stappen die u dient te volgen voor het opzetten van een IPsec XAuth VPN verbinding vanaf een macOS device. IPsec XAuth maakt gebruik van UDP 500 & 4500, indien de DrayTek geen publiek IP-adres op de WAN poort ontvangt dient u ervoor te zorgen dat deze poorten open staan naar het WAN IP-adres van de DrayTek.

Er zal een algemene IPsec XAuth User Pre-Shared-Key nodig zijn, deze kunt u in de DrayTek instellen bij VPN and Remote Access >> IPsec General Setup.

**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**

Certificate:

Preferred Local ID:

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  
DH Group: G21/G20/G19/G14/G5/G2/G1  
AH:  Enable

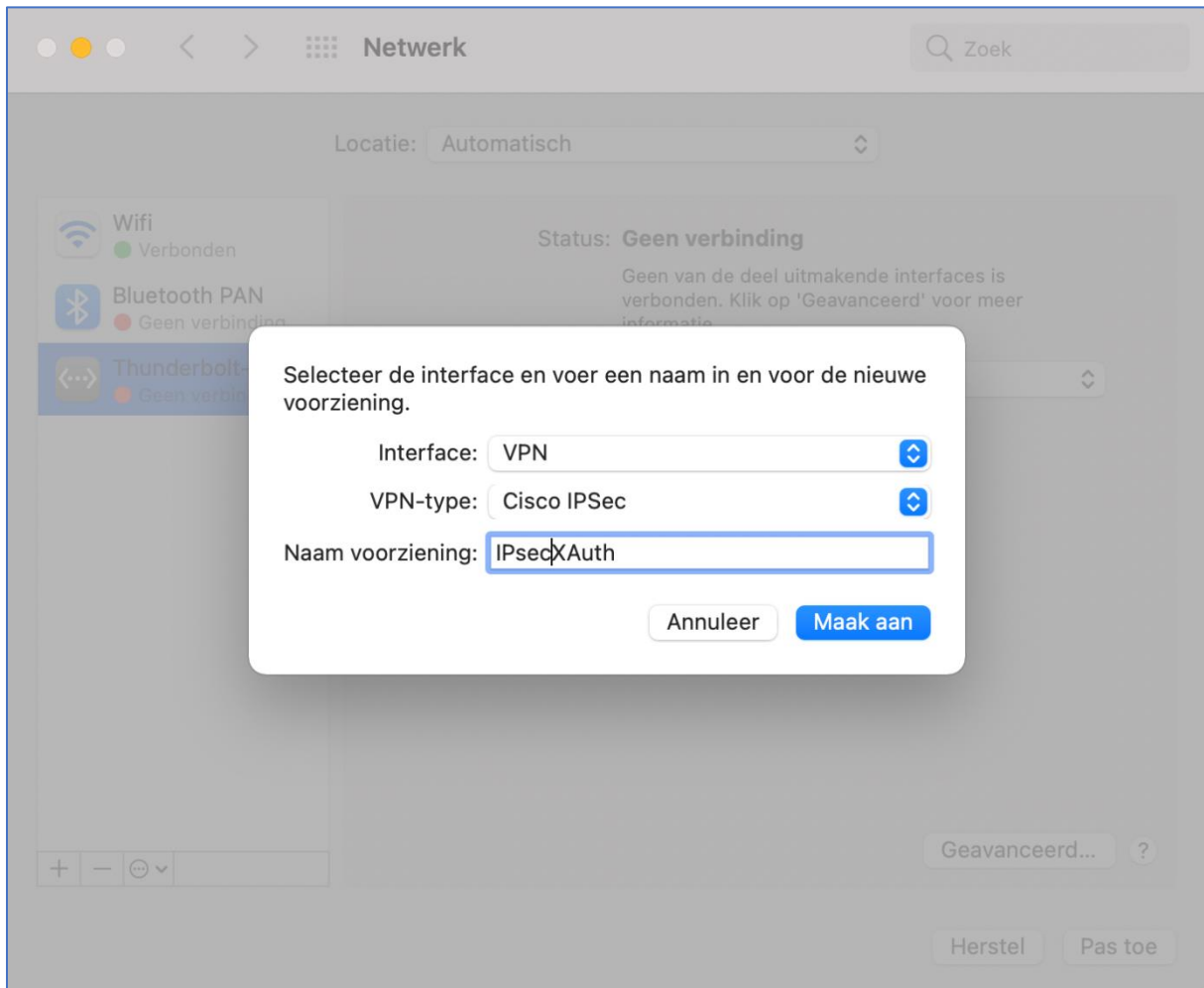
Vervolgens dient u één of meerdere VPN Remote Dial In Users aan te maken, per VPN gebruiker kunt u een eigen account aanmaken zodat iedere gebruiker zijn eigen gebruikersnaam en wachtwoord kan gebruiken.

**Index No. 17**

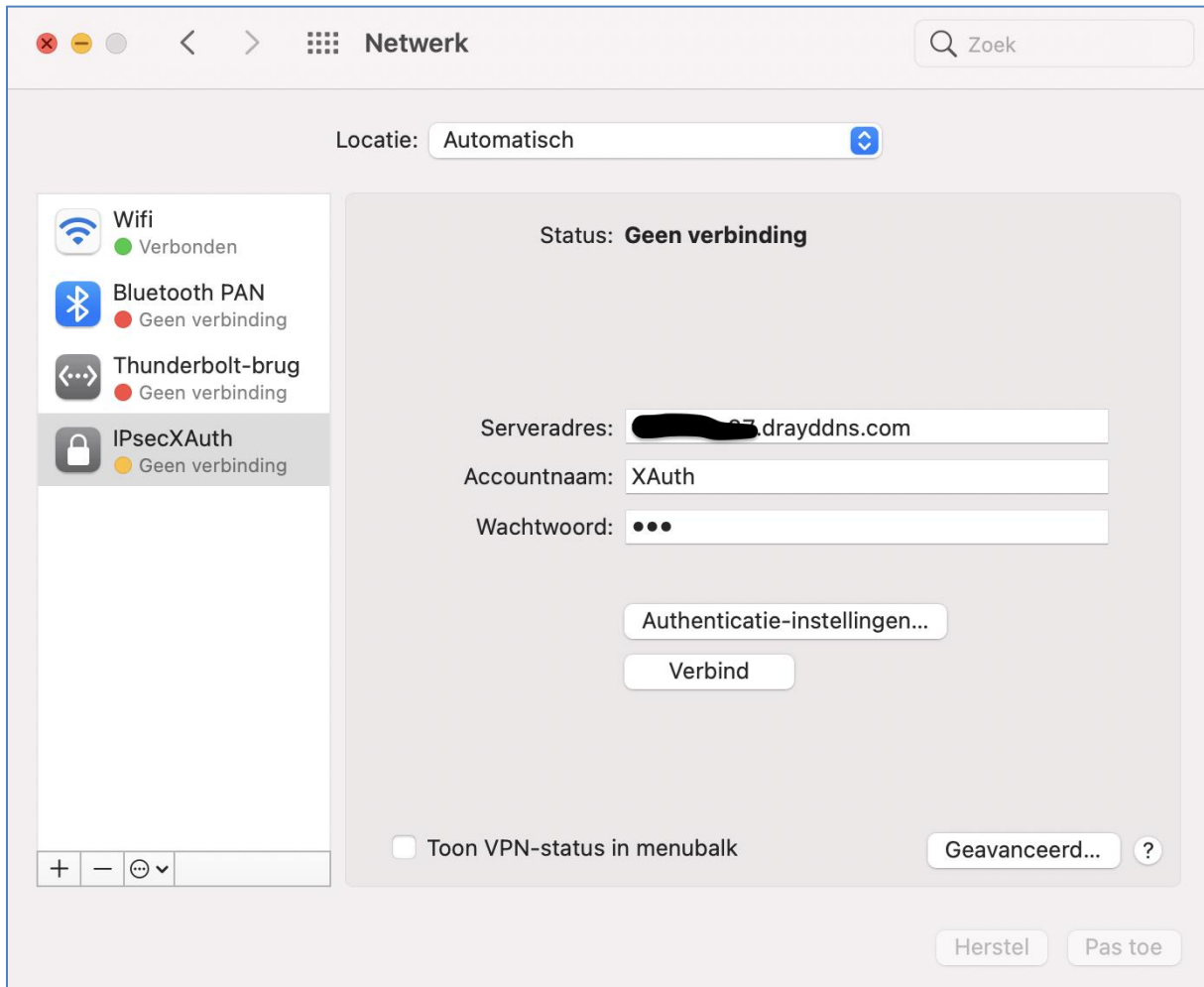
<p><b>User account and Authentication</b></p> <p><input checked="" type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <hr/> <p><b>Allowed Dial-In Type</b></p> <p><input type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input type="checkbox"/> IKEv1/IKEv2 <input type="checkbox"/> IKEv2 EAP <input checked="" type="checkbox"/> IPsec XAuth</p> <p><input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input type="checkbox"/> SSL Tunnel</p> <p><input type="checkbox"/> OpenVPN Tunnel</p> <hr/> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP <input type="text"/></p> <p>or Peer ID <input type="text" value="Max: 128 characters"/></p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p> <p>Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block <small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small></p> <hr/> <p><b>Subnet</b></p> <p><input type="text" value="LAN 1"/></p> <p><input type="checkbox"/> Assign Static IP Address</p> <p><input type="text" value="0.0.0.0"/></p>	<p>Username <input type="text" value="XAuth"/></p> <p>Password <input type="password" value="..."/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input type="text"/></p> <p>Secret <input type="text"/></p> <hr/> <p><b>IKE Authentication Method</b></p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p><input type="text" value="IKE Pre-Shared Key"/> <input type="text" value="Max: 128 characters"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p> <hr/> <p><b>IPsec Security Method</b></p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID (optional) <input type="text"/></p>
---	--

## VPN configuratie macOS

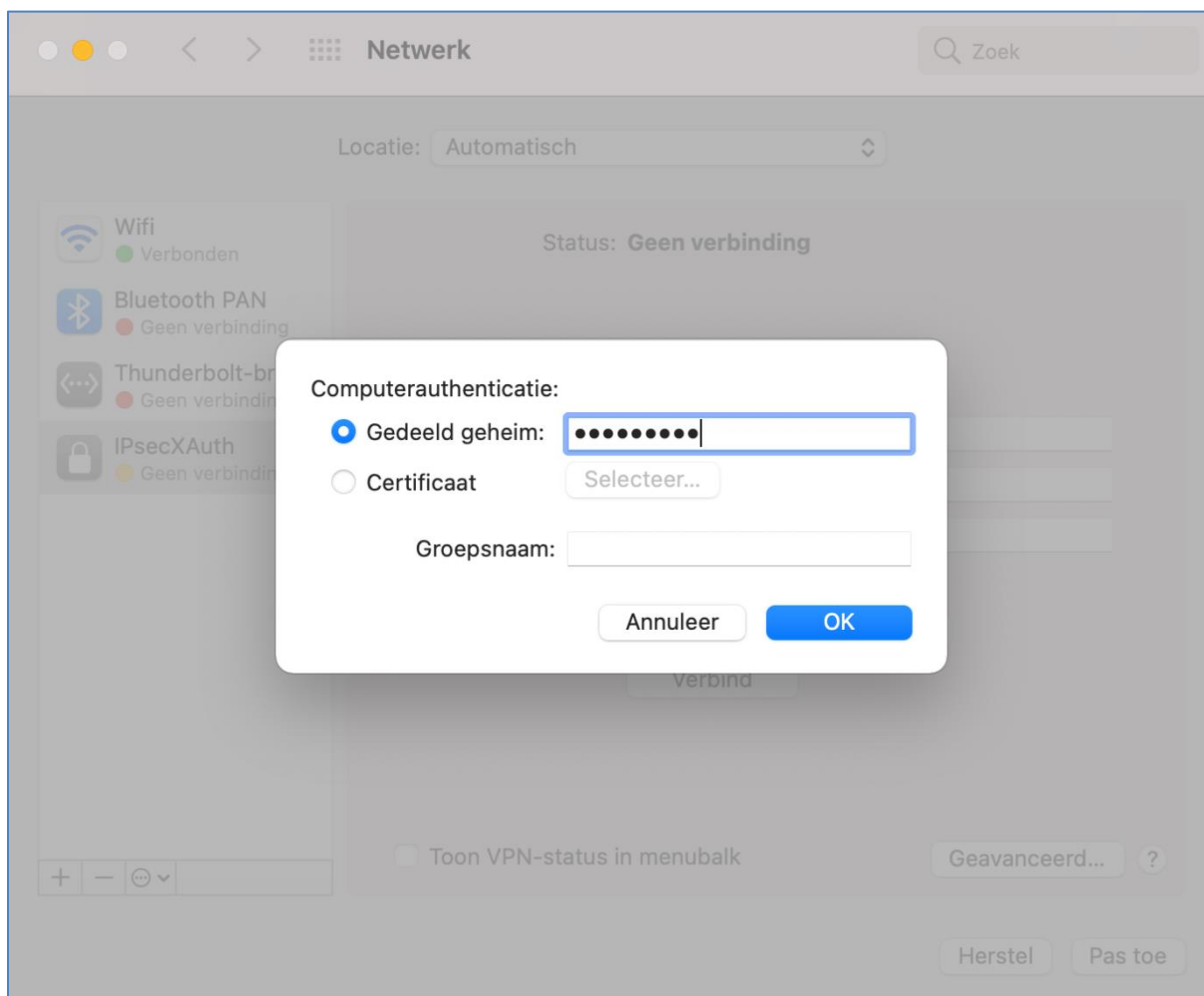
Op uw Mac kunt u bij **Systeem Instellingen > Netwerk** een nieuwe VPN verbinding aanmaken. Bij VPN type kiest u voor **Cisco IPSec**, daarnaast geeft u de VPN verbinding een naam.



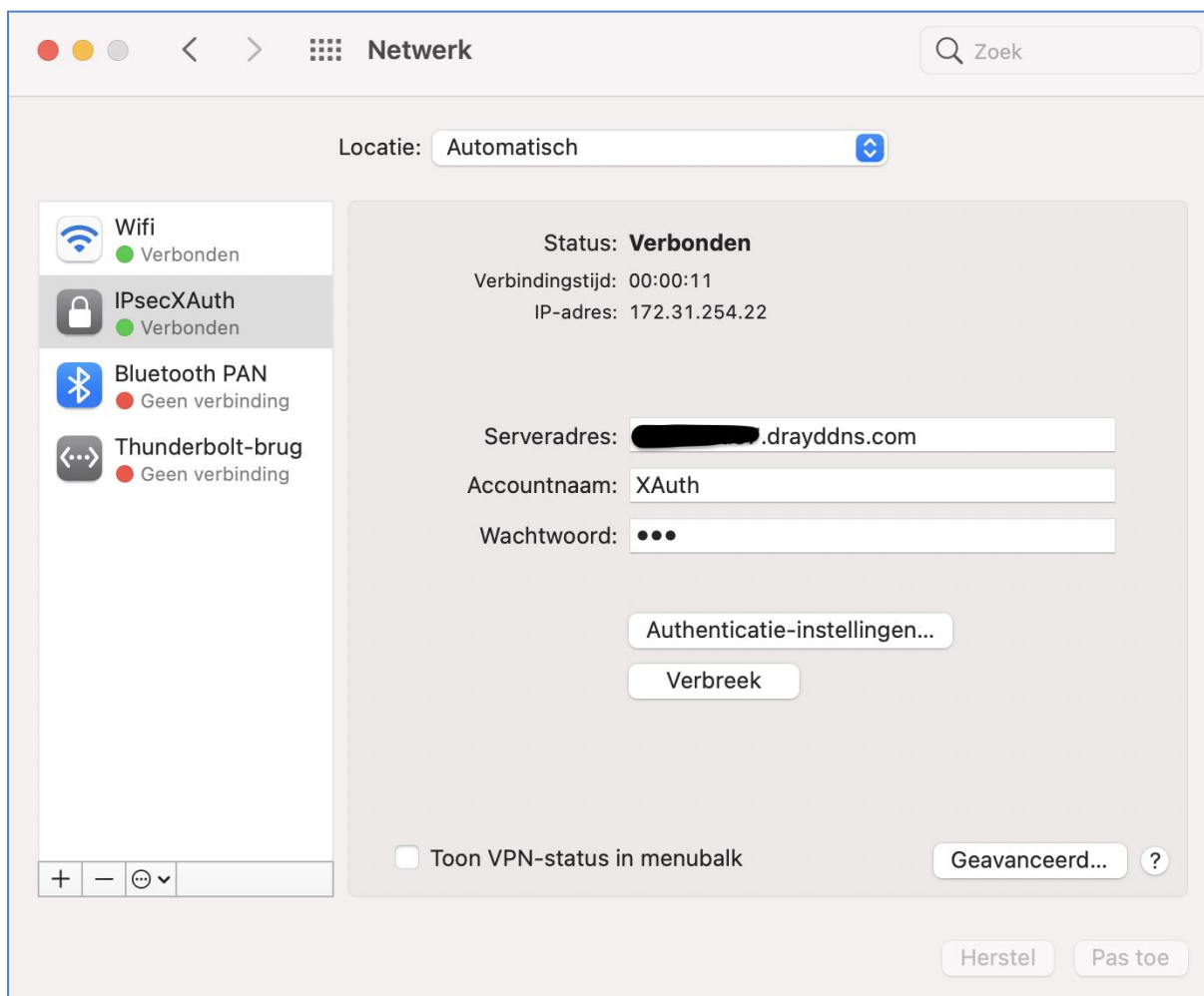
Bij Serveradres vult u het publieke IP-adres/DNS naam van de VPN server in. Vervolgens geeft u bij Accountnaam en Wachtwoord de login credentials op van de VPN gebruiker die u zojuist heeft aangemaakt.



Als laatste dient u de IPsec Xauth Pre-Shared Key nog op te geven, dit kan door op Authenticatie-instellingen te klikken. Vul bij Gedeeld geheim de Pre-Shared Key in en klik op OK.



Klik op Connect om de VPN verbinding op te bouwen. In onderstaand screenshot ziet u een actieve IPsec XAuth verbinding vanaf een macOS device naar de DrayTek modem/router.





### **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**

© 2021 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.