

DrayTek

DrayOS5

IPsec XAuth - macOS



Inhoudsopgave

IPsec XAuth	3
XAuth User PSK.....	4
Teleworker VPN instellingen	5
General.....	6
User Information	6
Teleworker VPN	7
Local IP Assignment	7
macOS setup.....	8
Smart-VPN setup	10

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 eigen gebruikersnaam en wachtwoord. 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.

Dit artikel demonstreert hoe je een DrayOS 5 Vigor Router configureert als een VPN-server voor IPsec Xauth-clients, en welke configuratie vereist is op macOS om de VPN op te zetten. In het voorbeeld wordt de Vigor2136 router gebruikt.

XAuth User PSK

IPsec Xauth maakt gebruik van één algemene pre-shared key, deze kunt u configureren bij VPN > General Setup.

DrayTek Vigor2136ax

VPN / General Setup

General Setup

IPsec WireGuard OpenVPN

Enabled

Authentication Settings for Dynamic Peer

Certificate Default_Certificate

Preferred Local ID Alternative Subject Name

General User PSK

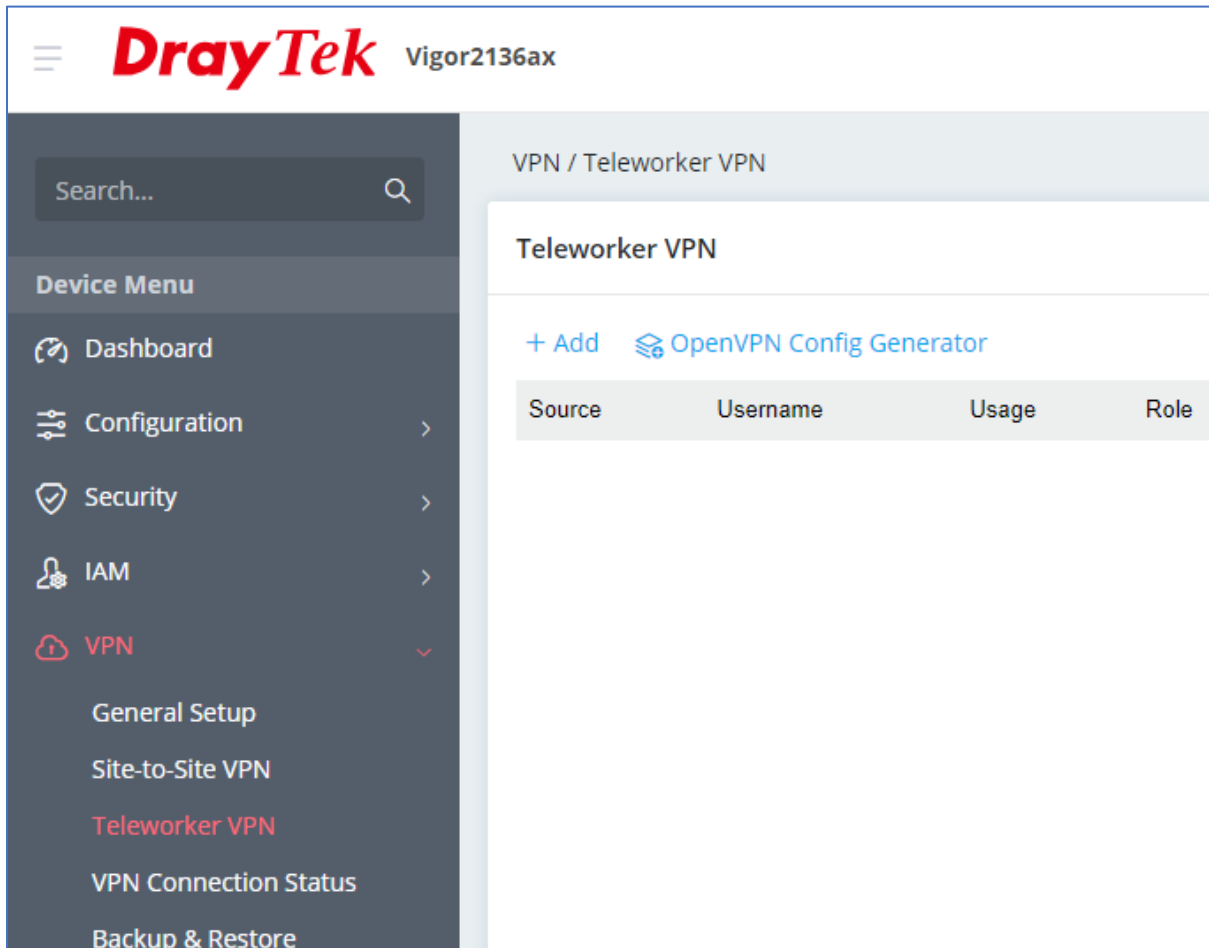
Pre-Shared Key

XAuth User PSK

Pre-Shared Key

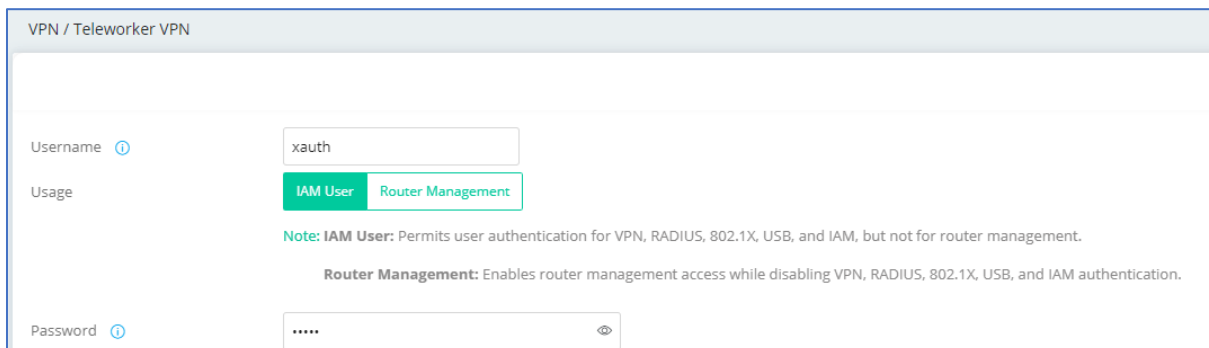
Teleworker VPN instellingen

Voor het aanmaken van een VPN account kunt u bij Teleworker VPN een nieuw account toevoegen om op + Add te klikken.



The screenshot shows the DrayTek Vigor2136ax web interface. The left sidebar contains a 'Device Menu' with options: Dashboard, Configuration, Security, IAM, VPN (highlighted), General Setup, Site-to-Site VPN, Teleworker VPN, VPN Connection Status, and Backup & Restore. The main content area is titled 'VPN / Teleworker VPN' and shows a 'Teleworker VPN' section with a '+ Add' button and an 'OpenVPN Config Generator' link. Below this is a table with columns: Source, Username, Usage, and Role.

Geef vervolgens een username en password op, selecteer IAM user om gebruik te kunnen maken van VPN.



The screenshot shows the configuration form for a Teleworker VPN user. The form includes the following fields and options:

- Username:** xauth
- Usage:** IAM User (selected), Router Management
- Password:** (masked with dots)

Note: IAM User: Permits user authentication for VPN, RADIUS, 802.1X, USB, and IAM, but not for router management.

Router Management: Enables router management access while disabling VPN, RADIUS, 802.1X, USB, and IAM authentication.

General

Naast het in en uitschakelen van een VPN profiel kunt u hier tevens een group policy koppelen aan het VPN account. Daarnaast kunt u een verval datum koppelen aan het VPN profiel. De Group Policy kunt u verder inrichten in het IAM menu, raadpleeg hiervoor de IAM handleiding op onze website voor meer informatie.

Status	Active	▼
Group Policy	None	▼
Expiration Time	Never	▼

User Information

Per gebruikers account kunt u e-mail adres of 06-nummer achterlaten. Deze informatie kan gebruikt worden wanneer u gebruik maakt van MFA. Indien u hier gebruik van wilt maken dient u een koppeling te hebben met een SMTP server of SMS provider, verder configuratie is mogelijk onder Configuration > Notification Services.

User Information	
Enable Email	<input checked="" type="checkbox"/>
Email	<input type="text"/>
	<input checked="" type="checkbox"/> Send Email Notification to the newly created User
Enable SMS	<input checked="" type="checkbox"/>
SMS	<input type="text"/>

Teleworker VPN

Hier activeert u het VPN profiel voor dit account, daarnaast kunt u hier aangeven welke VPN protocollen gebruikt kunnen worden om een VPN tunnel op te bouwen. We selecteren in dit geval enkel IPsec XAuth.

General **Teleworker VPN**

General

Enable Teleworker VPN

Idle Timeout (Seconds) ⓘ

VPN Schedule Always On Scheduled On

Download SmartVPN Client [Download SmartVPN Client](#)

Allowed VPN Protocols

Enable IPsec

Allowed IPsec Protocols IKEv1/v2 EAP XAuth

Enable WireGuard

Enable OpenVPN

Local IP Assignment

Bij Local IP Assignment kunt u de VPN client een vast IP-adres geven of de keuze op DHCP laten staan, de VPN client zal dan een IP-adres ontvangen van de DHCP server in de DrayTek.

Local IP Assignment

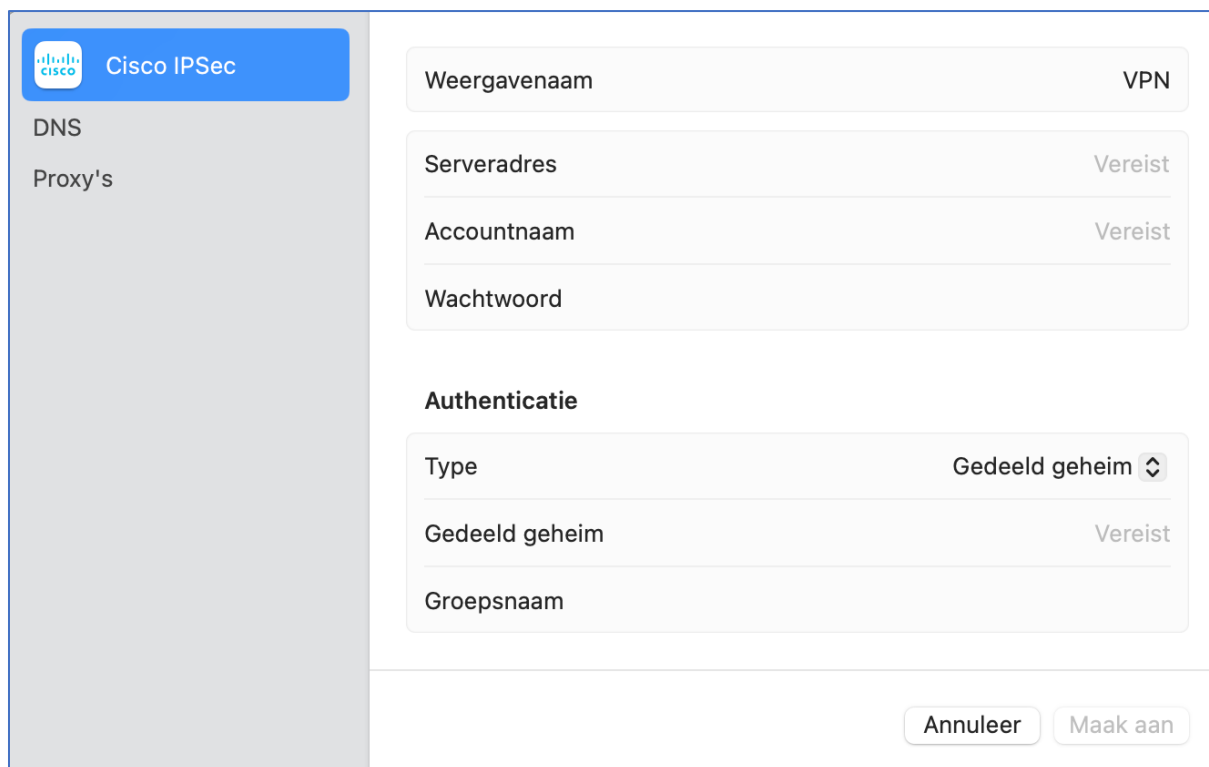
Assign IP By LAN DHCP Static IP

Assign IP from

Assign DNS By LAN DHCP Manually

macOS setup

Open de Systeeminstellingen op uw macOS apparaat en klik op VPN, hier kunt u een nieuw VPN-configuratie toevoegen. Voor IPsec XAuth selecteren we een Cisco IPsec profiel.



The screenshot shows the macOS System Settings window for a Cisco IPsec VPN profile. The left sidebar contains 'Cisco IPSec', 'DNS', and 'Proxy's'. The main area is divided into two sections: 'Weergavenaam' (VPN) and 'Authenticatie'. The 'Weergavenaam' section has fields for 'Serveradres' (Vereist), 'Accountnaam' (Vereist), and 'Wachtwoord'. The 'Authenticatie' section has a 'Type' dropdown set to 'Gedeeld geheim', a 'Gedeeld geheim' field (Vereist), and a 'Groepsnaam' field. At the bottom right are 'Annuleer' and 'Maak aan' buttons.

Belangrijke instellingen voor het inrichten van een XAuth VPN profiel:

Weergavenaam : Profiel naam

Serveradres : WAN IP-adres of hostname van de DrayTek

Accountnaam : Username welke is aangemaakt in de DrayTek

Wachtwoord : Wachtwoord welke is aangemaakt in de DrayTek

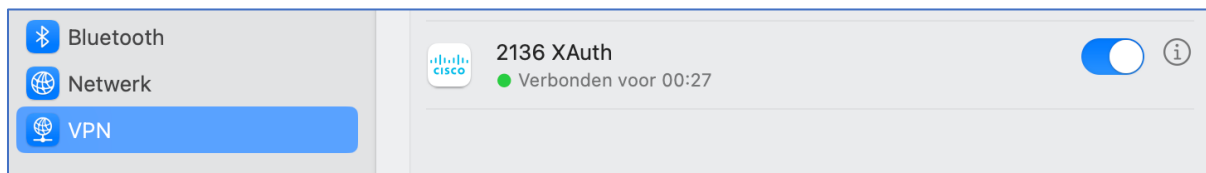
Authenticatie

Type : Selecteer Gedeeld geheim, dit komt overeen met de XAuth PSK in de DrayTek.

Gedeeld geheim : Voer hier de XAuth Pre Shared Key in die u hebt aangemaakt in de DrayTek.

Klik na het invullen van deze instellingen op Maak aan om het profiel op te slaan.

Het VPN profiel is nu beschikbaar voor gebruik, door op de slider te klikken kunt u het profiel activeren. Indien de instellingen overeenkomen zal de VPN tunnel online komen, zoals te zien is op onderstaande afbeelding.



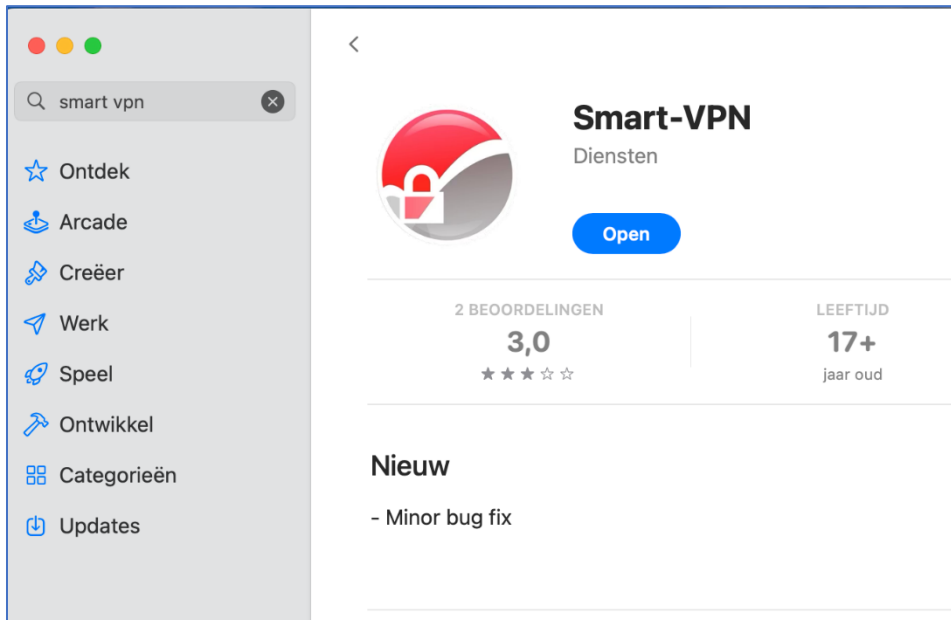
In de Vigor2136 kunt u onder VPN Connection Status de status inzien van de verbonden VPN gebruiker.

A screenshot of the Vigor2136 web interface showing the 'VPN / VPN Connection Status' page. The page has a search bar and a 'Refresh' button. Below the search bar, there are tabs for 'Site-to-Site VPN', 'Teleworkers VPN', 'Connection History', 'Failed VPN Connection Attempts', and 'Blocked by Brute Force Protection'. The 'Teleworkers VPN' tab is selected. Underneath, there is a section titled 'Active Teleworkers' with a search bar. A table lists active users with the following columns: Username, Authentication Type, Assigned IP, Remote IP, VPN Type, Interface, TX Rate, RX Rate, Uptime, and Option. One user is listed: 'xauth' with 'Local User' authentication, '172.31.254.201' assigned IP, 'public IP van de VPN client' remote IP, 'IPsec XAuth' VPN Type, '[WAN] WAN1' interface, '670 bps' TX Rate, '12.51 Kbps' RX Rate, and '00:00:10' uptime. There is a 'Drop' button in the Option column.

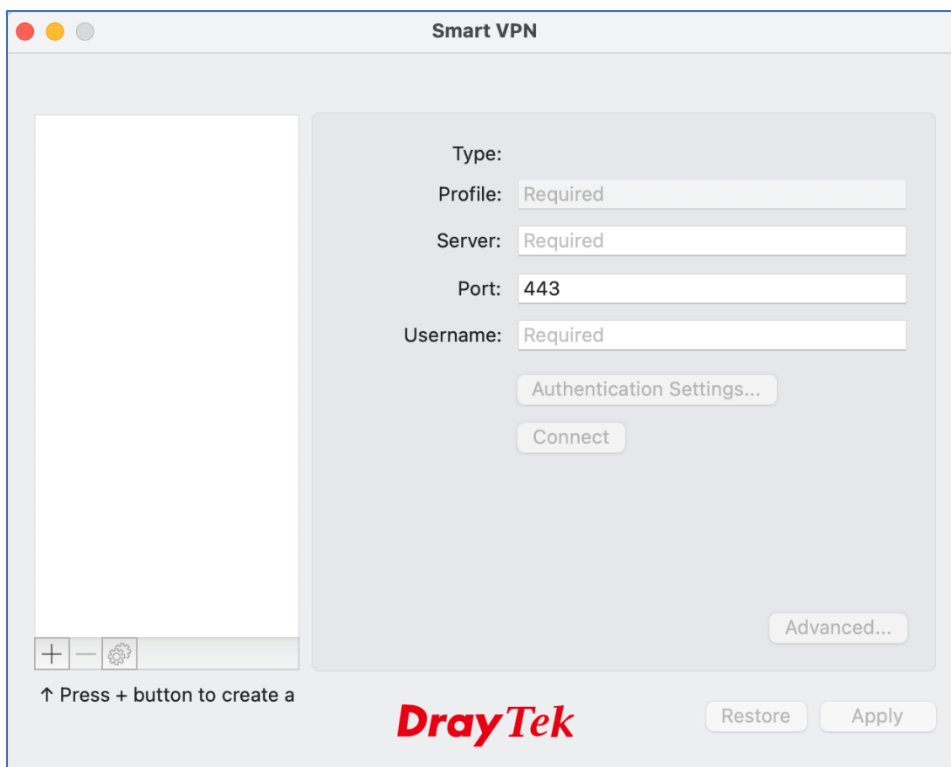
Username	Authentication Type	Assigned IP	Remote IP	VPN Type	Interface	TX Rate	RX Rate	Uptime	Option
xauth	Local User	172.31.254.201	public IP van de VPN client	IPsec XAuth	[WAN] WAN1	670 bps	12.51 Kbps	00:00:10	Drop

Smart-VPN setup

DrayTek heeft tevens een eigen VPN client beschikbaar voor macOS gebruikers, deze VPN client app kunt u gratis downloaden in de App Store op uw Apple device. Deze tool is beschikbaar voor zowel macOS als iOS.



Door op het + teken te klikken kunt u een nieuw VPN profiel inrichten.



Selecteer bij Type IPsec XAuth, vervolgens kunt u het profiel een naam geven. Bij Server geeft u het WAN IP-adres of Hostname in van de DrayTek. Bij User name kunt u de gebruikersnaam opgeven van de VPN Teleworker die u hebt aangemaakt.

Create a new Smart VPN profile:

Type:

Profile:

Server:

User name:

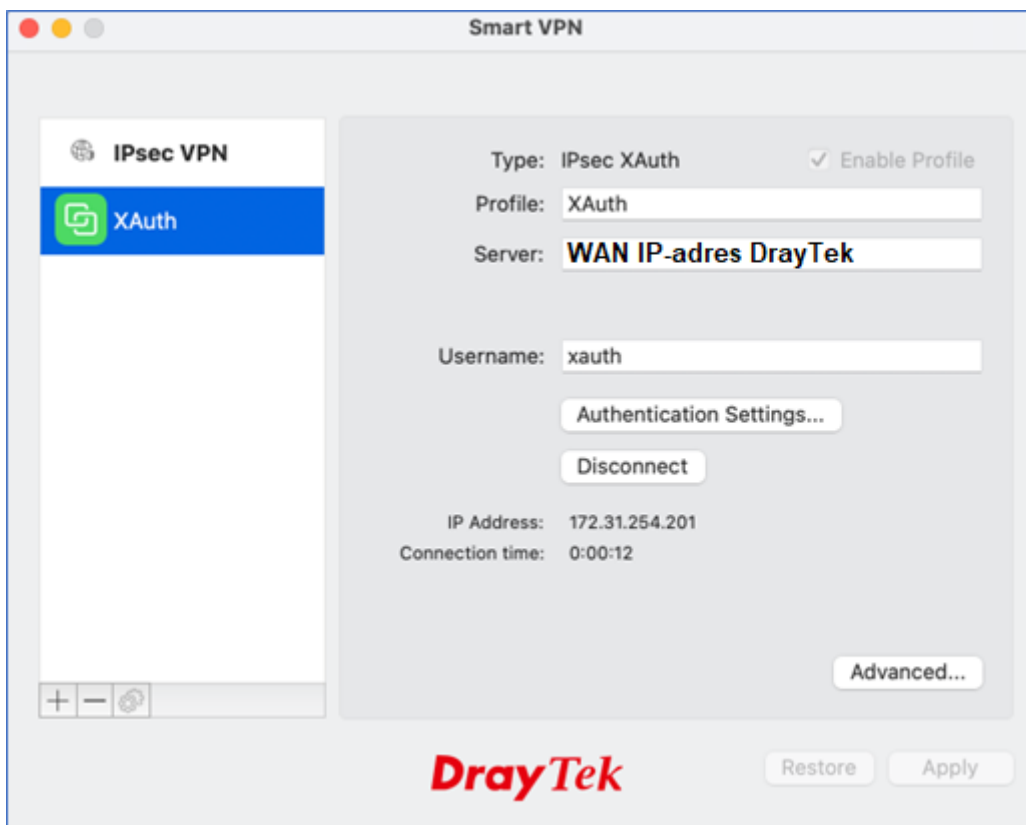
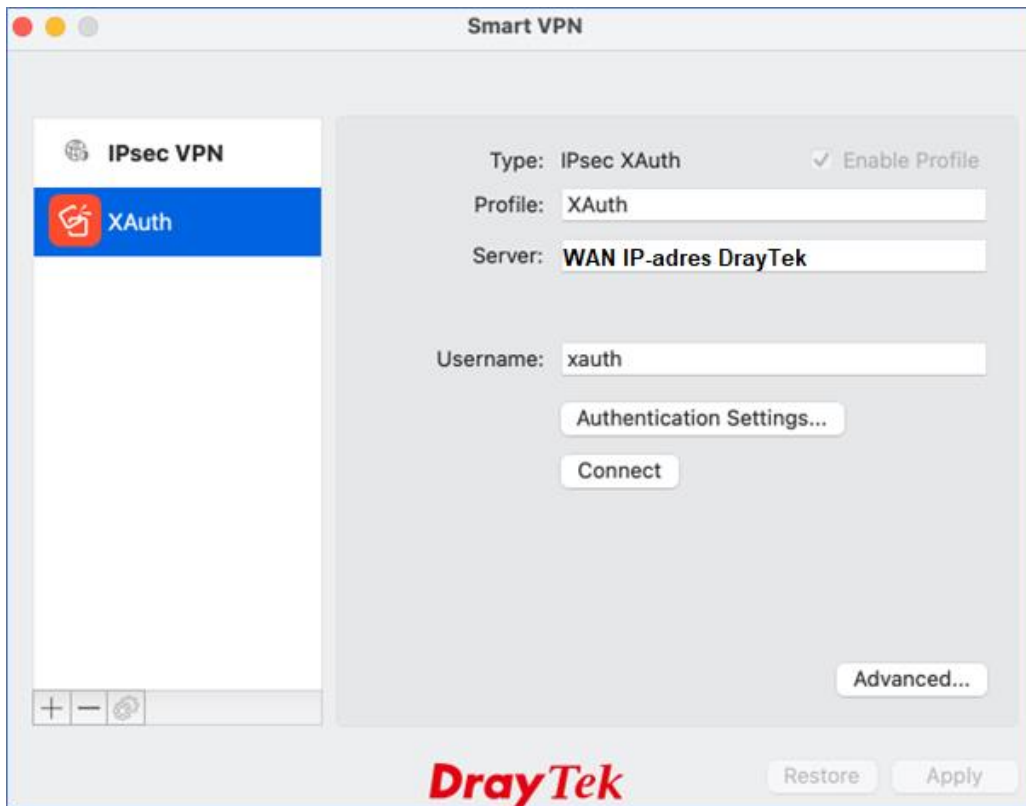
Klik vervolgens op Authentication om het wachtwoord en de XAuth pre-shared key in te vullen. Klik hierna op OK en op Create om het VPN profiel op te slaan.

User Authentication:

Password:

Shared Secret:

Activeer het profiel door Enable Profile aan te vinken, vervolgens kunt u op Connect klikken om de VPN tunnel op te bouwen.



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

© 2024 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.