DrayTek

*DrayOS5*

# *Multi Factor Authentication*

## Inhoudsopgave

## Multi Factor Authenticatie

Multi Factor Authenticatie is een beveiligingsmethode waarbij u meerdere verificatiestappen moet doorlopen om toegang te krijgen tot een systeem. Dit kan een combinatie zijn van iets wat u weet (zoals een wachtwoord), iets wat u hebt (zoals een telefoon) en iets wat u bent (zoals een vingerafdruk).

MFA verhoogt de beveiliging door extra lagen toe te voegen, waardoor het moeilijker wordt voor hackers om toegang te krijgen, zelfs als ze je wachtwoord kennen. Het is vooral belangrijk voor het beschermen van gevoelige gegevens en het voldoen aan beveiligingsnormen.

MFA wordt in DrayOS5 ondersteund voor zowel VPN-, LAN- als WAN-toegang. In deze handleiding behandelen we de configuratiemogelijkheden om uw DrayOS5-apparaat in te stellen voor Multi-Factor Authenticatie.

## Multi Factor Configuratie mogelijkheden

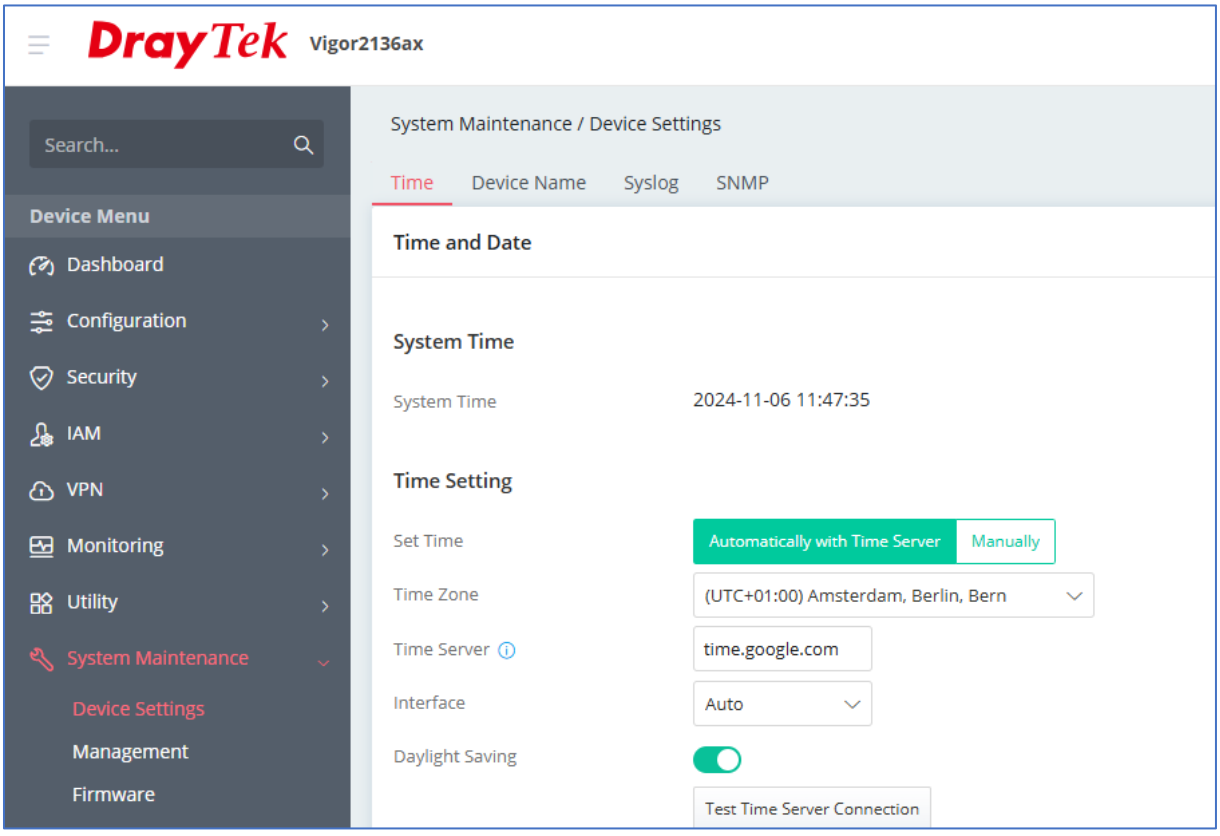
Op dit moment ondersteunen we onderstaande mogelijkheden voor MFA.
TOTP : Time Based One Time Password.
Email : Via een e-mail, SMTP koppeling met de server noodzakelijk.
SMS : Via een SMS, hiervoor is een SMS provider noodzakelijk.
mOTP : Mobile One Time Password, verouderde methode voor OTP.

De meest gebruiksvriendelijke manier om MFA toe te passen is via TOTP. Hiervoor kan de Google Authenticator-app of de Microsoft Authenticator-app worden gebruikt om de MFA-controle uit te voeren. Beide apps zijn gratis te downloaden in de appstore op uw smartphone.

## TOTP

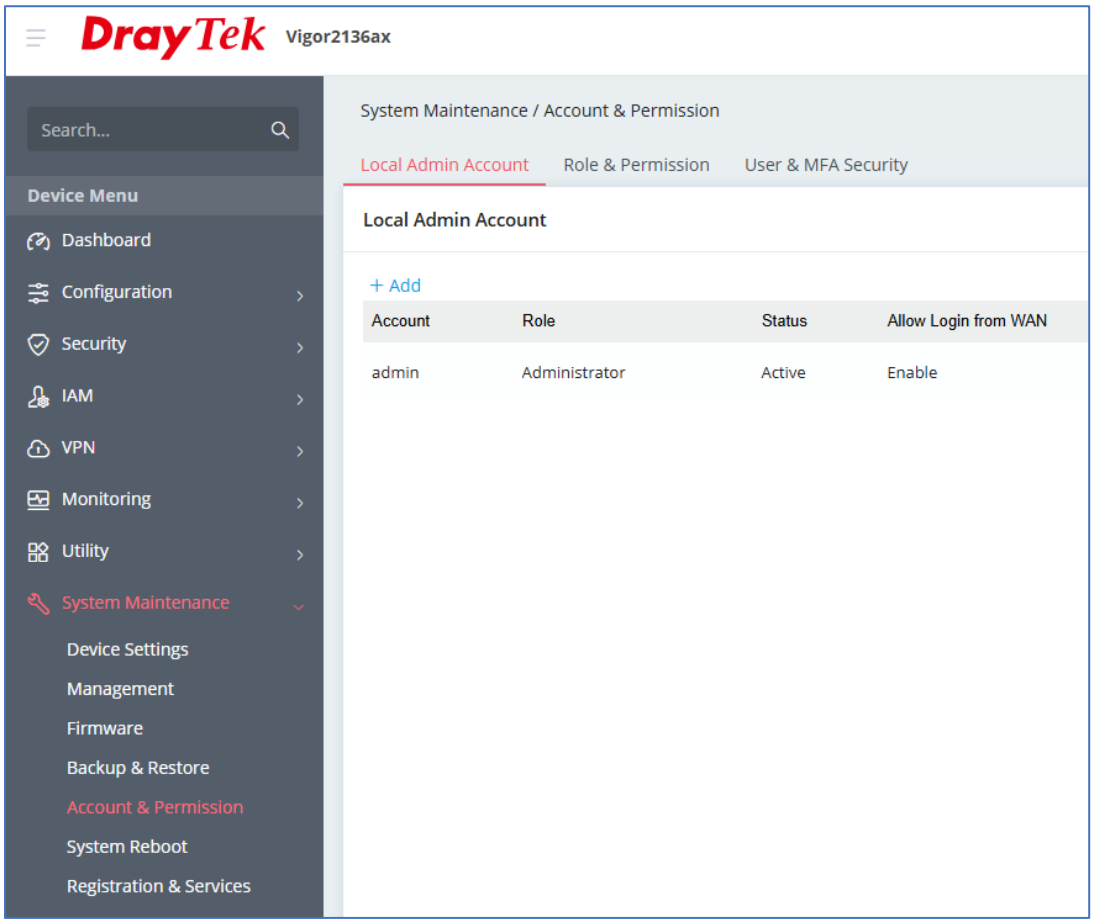
TOTP werkt door een code te genereren die gebaseerd is op de huidige tijd en een geheime sleutel. Daarom is het belangrijk dat de tijd op zowel de server als de client goed gesynchroniseerd is. Een significante tijdsverschil kan ervoor zorgen dat de gegenereerde codes ongeldig zijn.

De tijdinstellingen op de DrayTek kunt u controleren via het **System Maintenance > Device Settings**-menu. Zorg ervoor dat de DrayTek de juiste systeemtijd heeft.

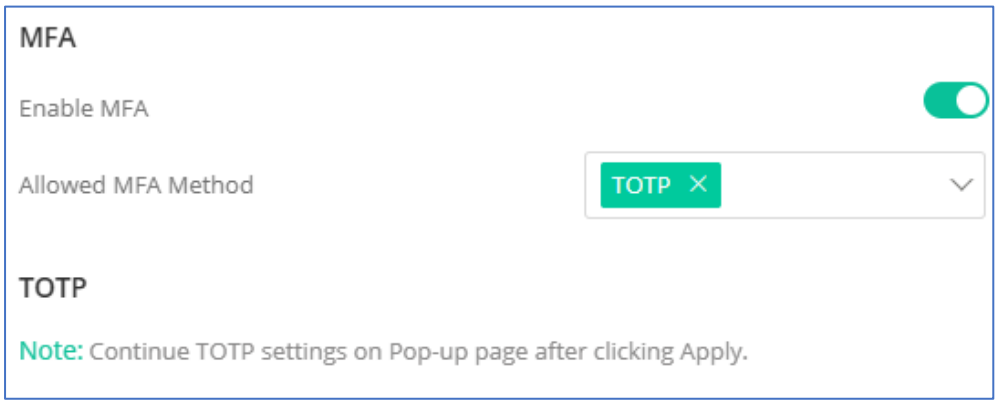


## Admin account met MFA

Standaard is uw admin-account niet beschermd met MFA. Om uw account te beveiligen, dient u onder **Account & Permissions** MFA in te schakelen voor de admin-gebruiker.



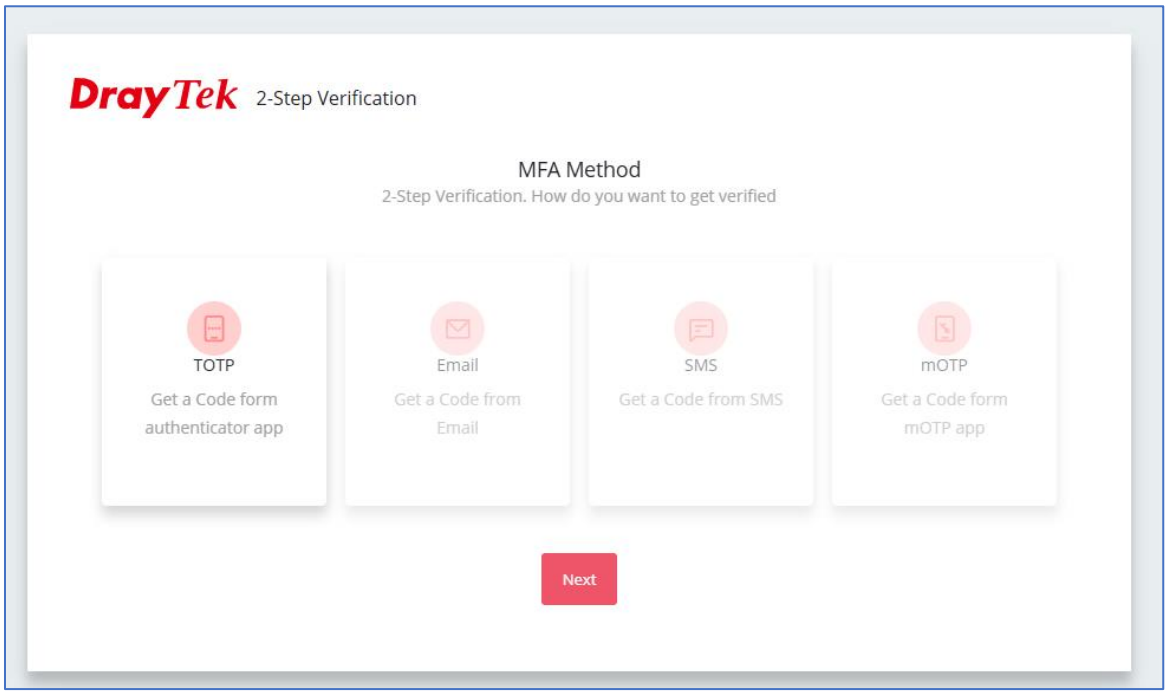

Klik op **Edit** om de configuratie-instellingen van de admin-gebruiker te openen. Activeer MFA en selecteer **TOTP** om de instellingen vervolgens op te slaan.



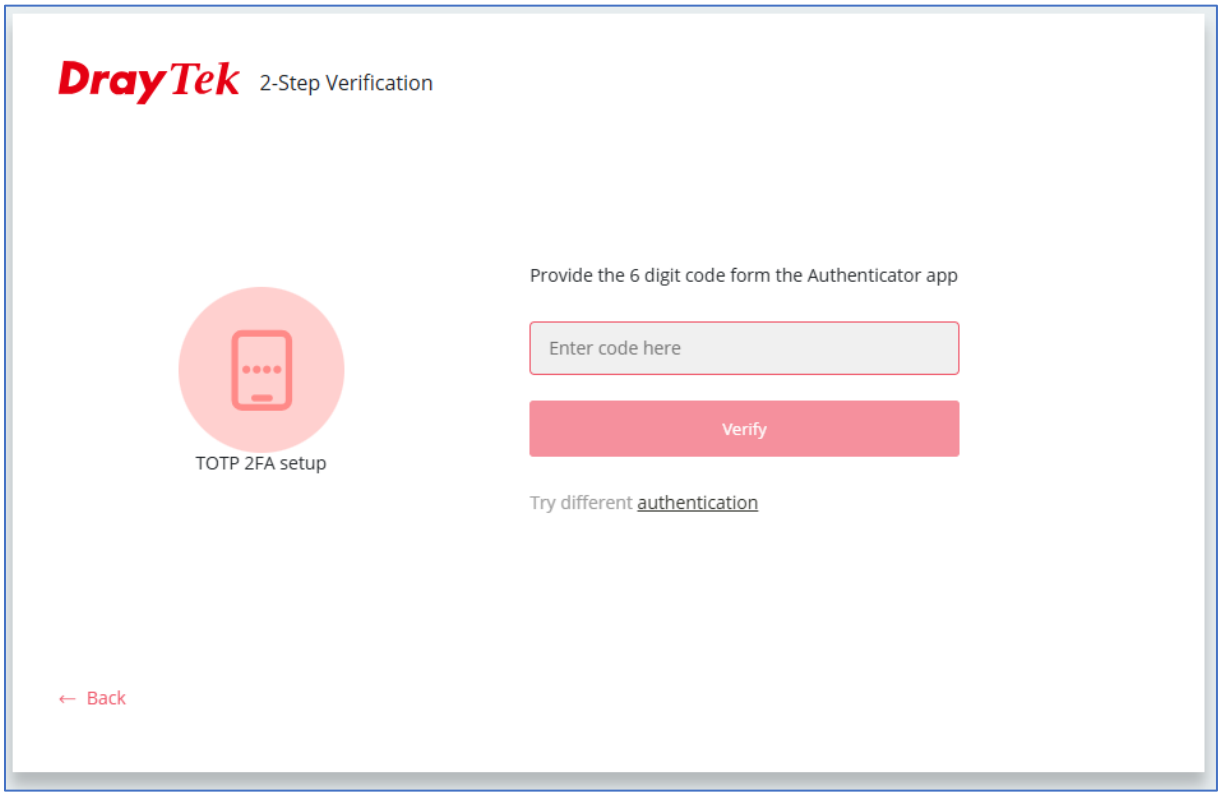
## TOTP verificatie

Nadat u op **Apply** hebt geklikt, verschijnt er een pop-up scherm met een TOTP Secret en QR-code. U kunt deze QR-code direct scannen met de Google Authenticator-app om de verificatiecode in te voeren.


Wanneer u de verificatiecode succesvol hebt ingevuld, kan de admin-gebruiker bij de volgende login gebruik maken van MFA.

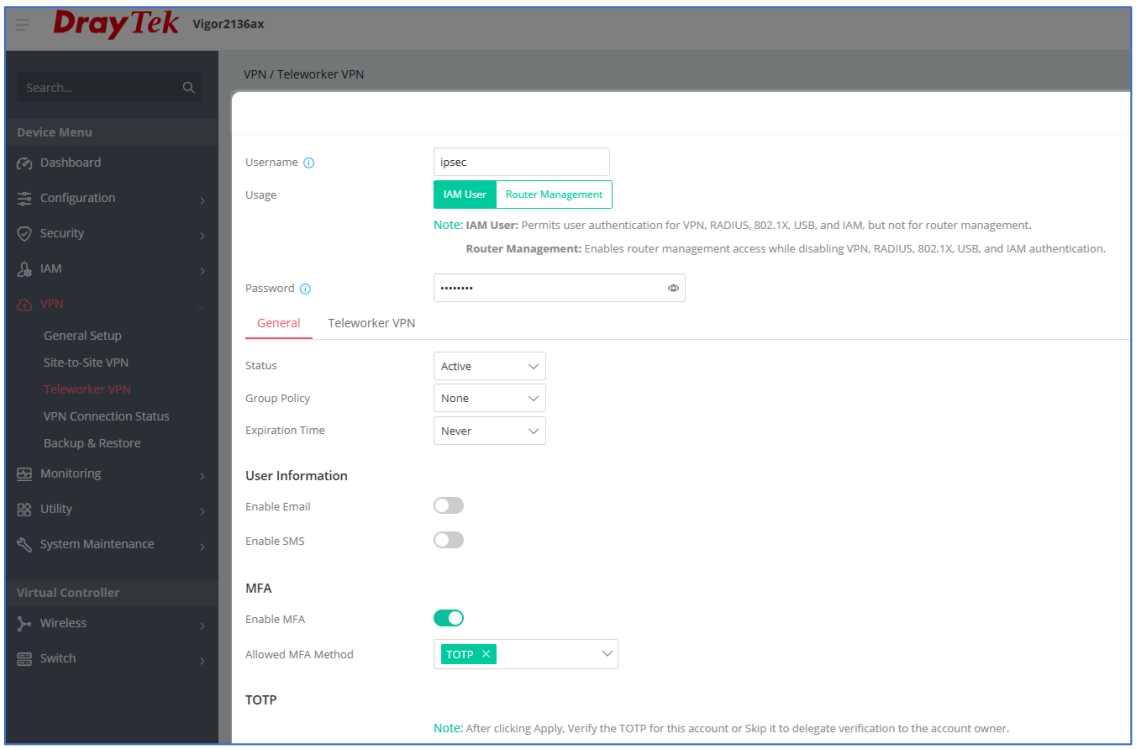


Vul de code in die u ziet in de Google Authenticator-app. Deze code is 30 seconden geldig en wordt elke 30 seconden vernieuwd.



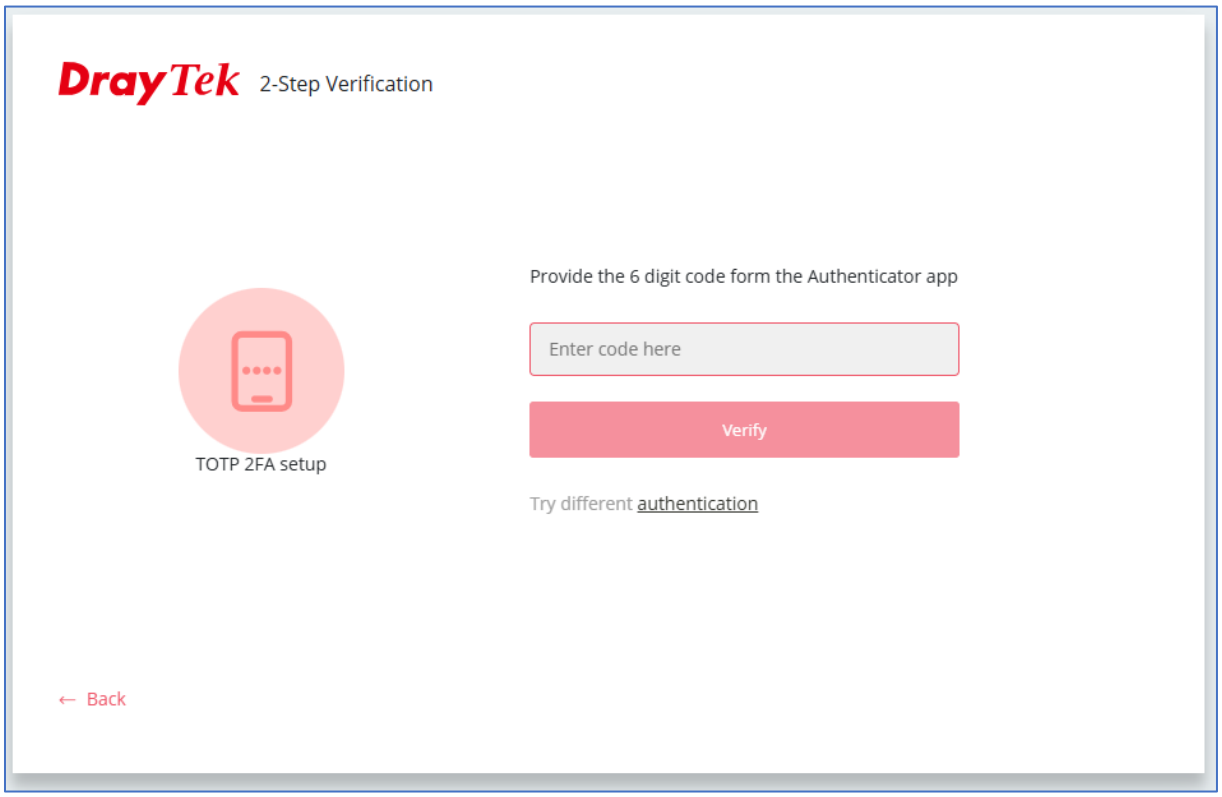
## VPN account met MFA

Per VPN account kan MFA worden ingeschakeld met daarin de diverse mogelijkheden die reeds zijn besproken in deze handleiding. Ook voor het gebruik van MFA icm VPN adviseren wij TOTP.



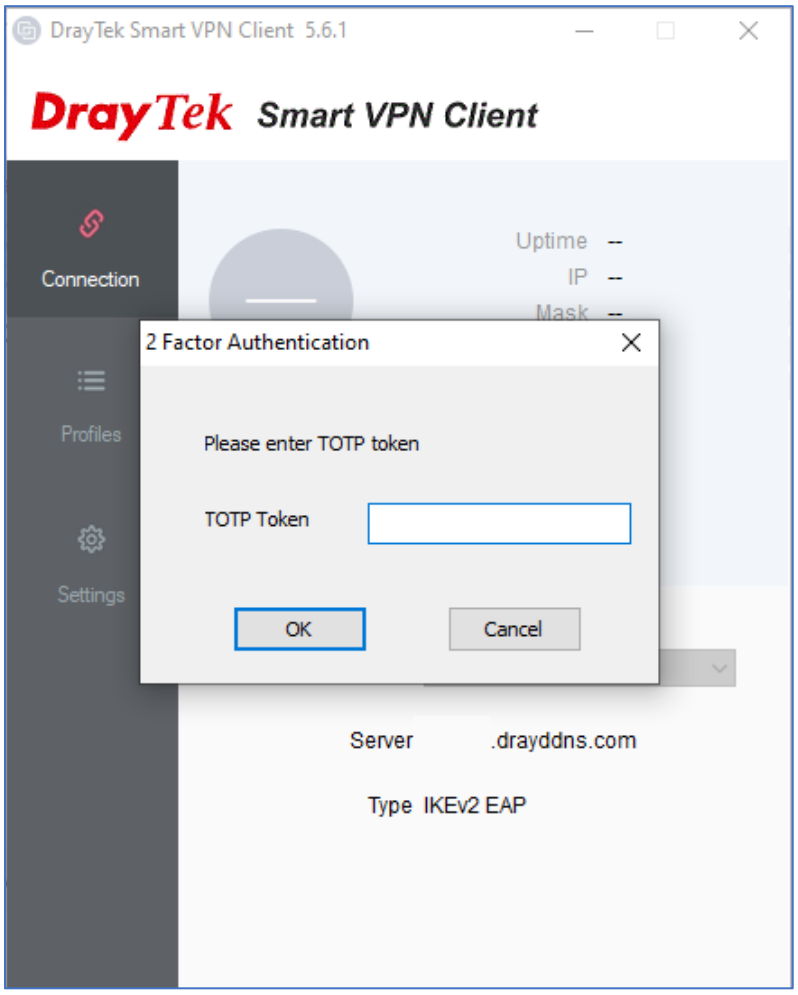

Nadat u MFA hebt ingeschakeld en TOTP hebt geselecteerd klikt u op Apply om het profiel op te slaan. U krijgt vervolgens direct de QR code te zien die nodig is voor de validation. Scan deze code met uw Google Authenticator app voor de validation code.

Bij het opzetten van de VPN-tunnel verschijnt een melding voor 2-step verification wanneer u een IP-adres in het LAN-subnet van de DrayTek benadert. De MFA voorkomt hiermee directe toegang tot apparaten in het LAN-netwerk van de DrayTek. Pas na een succesvolle MFA-verificatie is toegang tot het LAN-netwerk mogelijk.



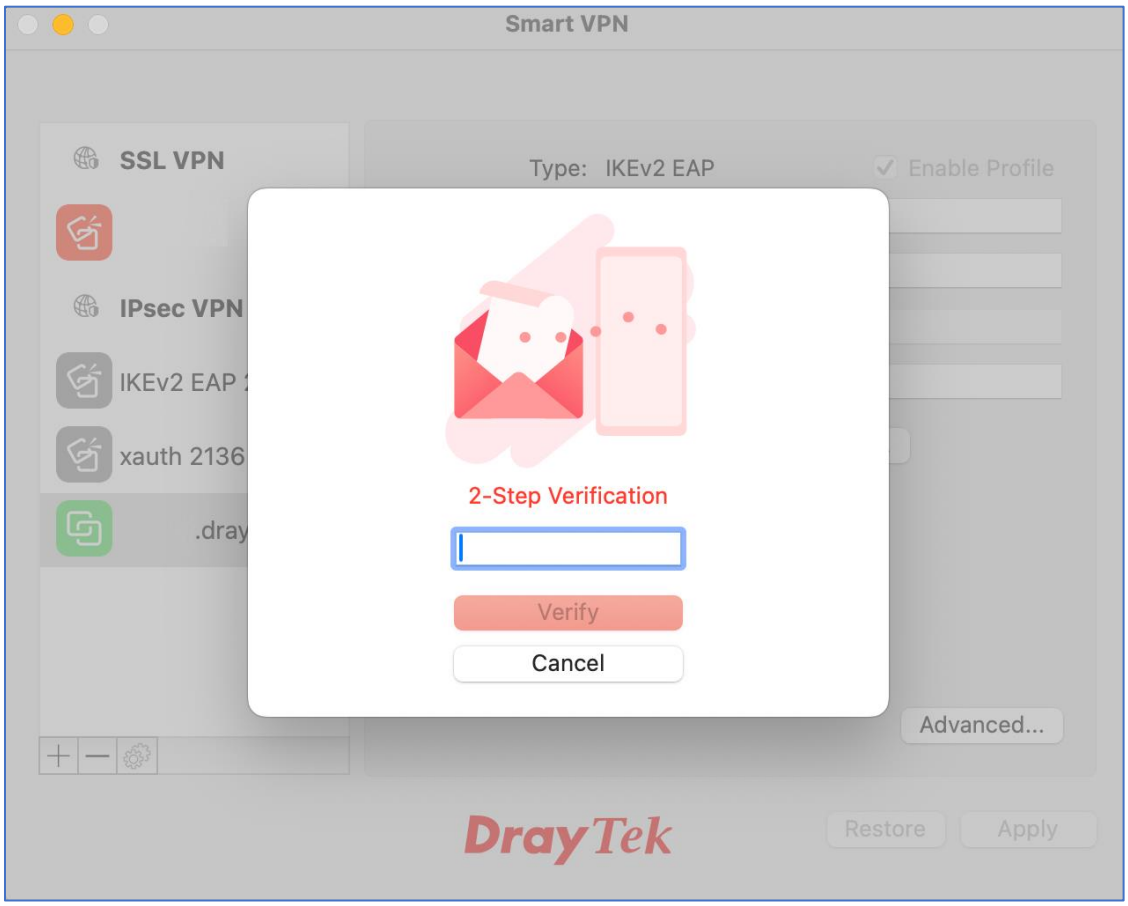
## MFA via Smart VPN Client (Windows)

De Smart VPN Client van DrayTek ondersteund tevens MFA, deze client detecteert automatisch of de VPN server MFA vereist. De gebruiker zal na het opzetten van de VPN tunnel een popup scherm zien waarin de TOTP token ingevuld kan worden.



## MFA via Smart VPN app (macOS)

DrayTek heeft tevens een Smart VPN app beschikbaar in de appstore welke u kunt gebruiken om een VPN tunnel op te bouwen. Deze smart VPN app detecteert tevens of er een MFA vereist is.



**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.