

DrayTek

DrayOS5
Multi Factor Authentication



Inhoudsopgave

Multi Factor Authenticatie	3
Multi Factor Configuratie mogelijkheden	4
TOTP	4
Admin account met MFA	5
TOTP verificatie.....	6
VPN account met MFA.....	8
MFA via Smart VPN Client (Windows)	10
MFA via Smart VPN app (macOS).....	11

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.

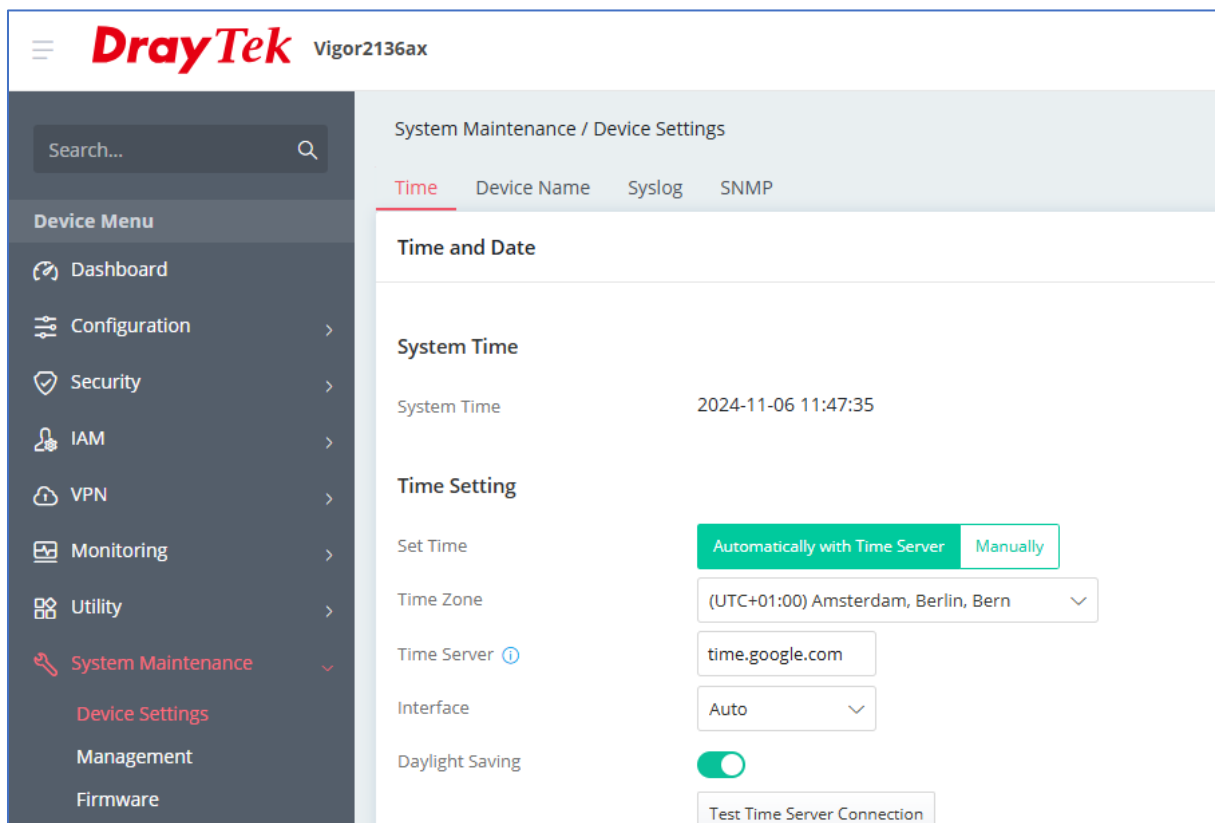
mOTP : Mobile One Time Password, verouderde methode voor OTP.

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.

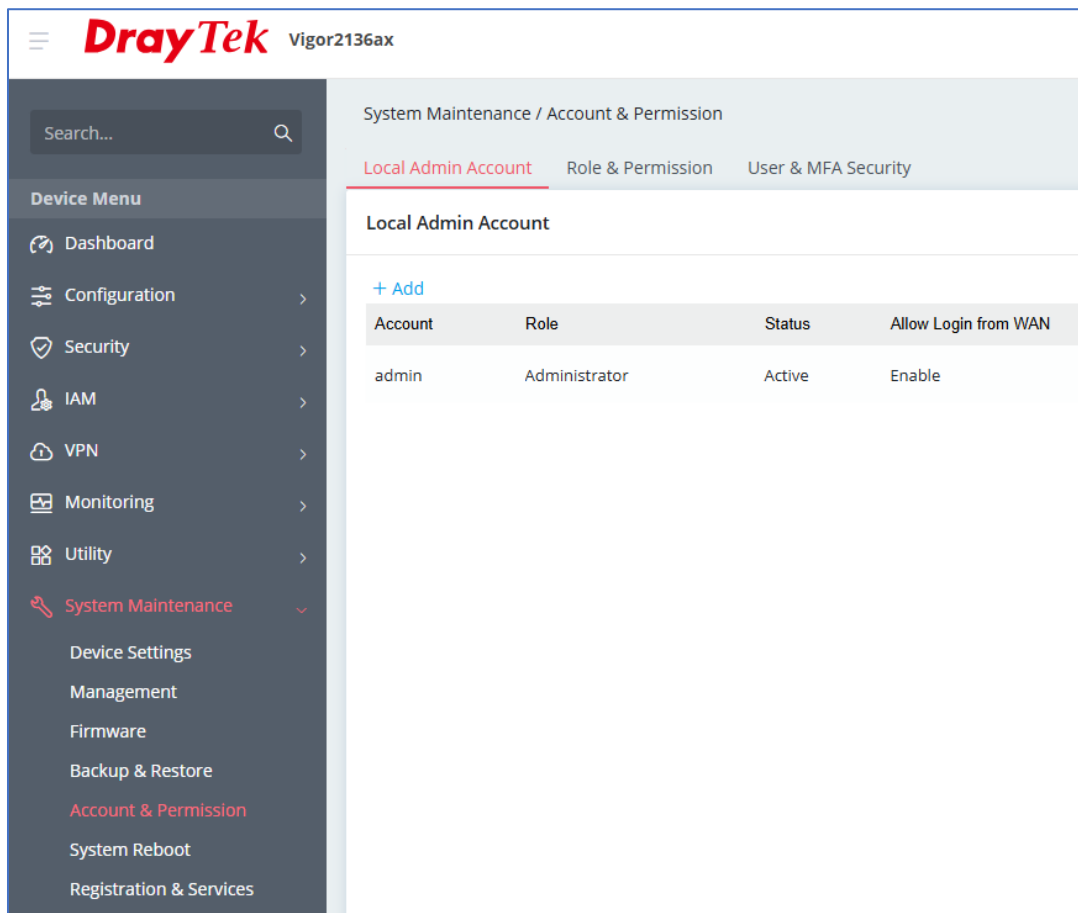
De tijdstellingen op de DrayTek kunt u controleren via het **System Maintenance > Device Settings**-menu. Zorg ervoor dat de DrayTek de juiste systeemtijd heeft.



The screenshot displays the DrayTek Vigor2136ax web interface. The left sidebar shows the 'Device Menu' with 'System Maintenance' selected, leading to 'Device Settings'. The main content area is titled 'System Maintenance / Device Settings' and has tabs for 'Time', 'Device Name', 'Syslog', and 'SNMP'. The 'Time' tab is active, showing 'Time and Date' settings. The 'System Time' is displayed as 2024-11-06 11:47:35. Under 'Time Setting', there are options for 'Set Time' (Automatically with Time Server or Manually), 'Time Zone' (UTC+01:00 Amsterdam, Berlin, Bern), 'Time Server' (time.google.com), 'Interface' (Auto), and 'Daylight Saving' (enabled). A 'Test Time Server Connection' button is also present.

Admin account met MFA

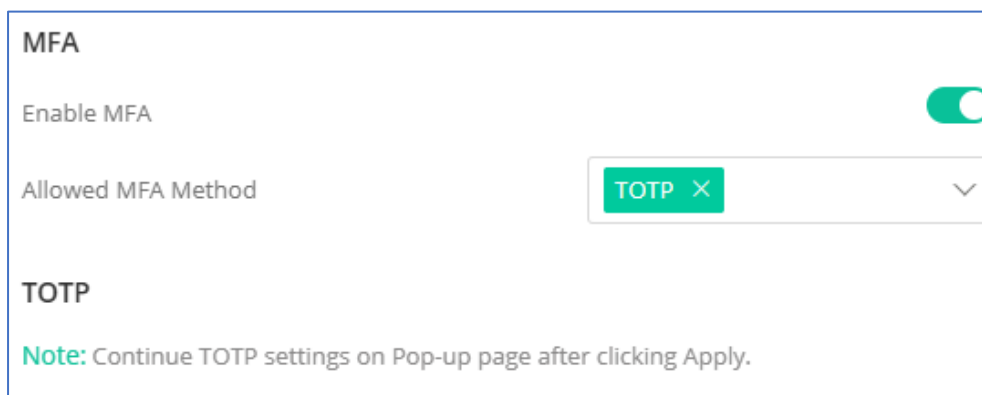
Standaard is uw admin-account niet beschermd met MFA. Om uw account te beveiligen, dient u onder **Account & Permissions** MFA in te schakelen voor de admin-gebruiker.



The screenshot shows the DrayTek Vigor2136ax web interface. The left sidebar contains a 'Device Menu' with options like Dashboard, Configuration, Security, IAM, VPN, Monitoring, Utility, System Maintenance (selected), Device Settings, Management, Firmware, Backup & Restore, Account & Permission, System Reboot, and Registration & Services. The main content area is titled 'System Maintenance / Account & Permission' and has three tabs: 'Local Admin Account' (selected), 'Role & Permission', and 'User & MFA Security'. Below the tabs, there is a section for 'Local Admin Account' with a '+ Add' button and a table listing the admin account.

Account	Role	Status	Allow Login from WAN
admin	Administrator	Active	Enable

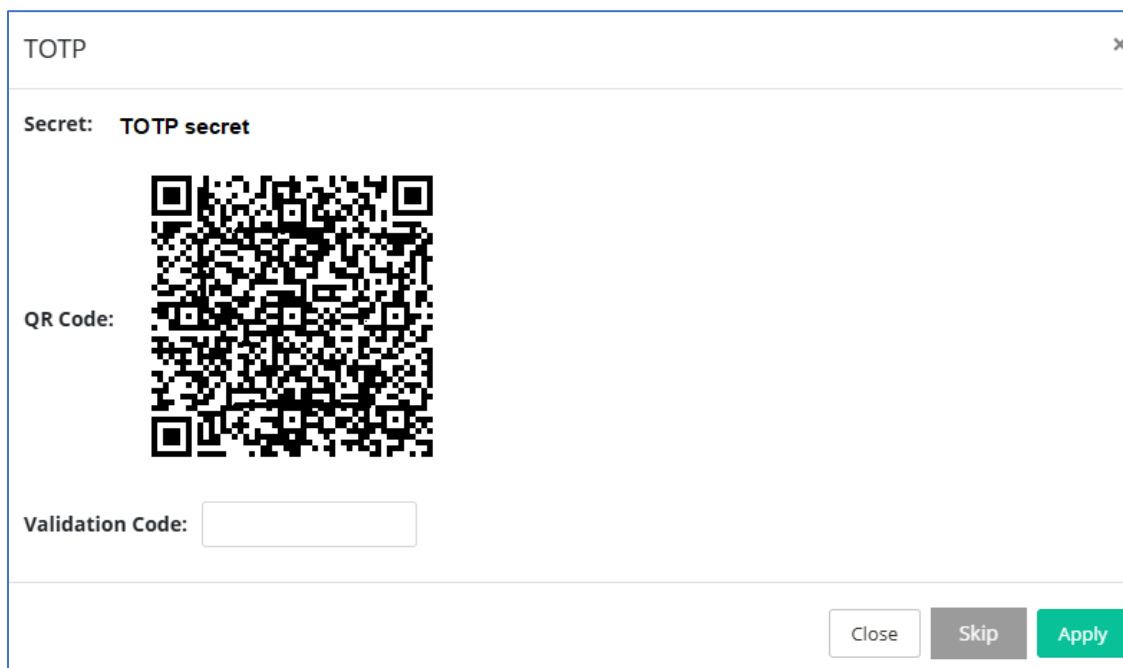
Klik op **Edit** om de configuratie-instellingen van de admin-gebruiker te openen. Activeer MFA en selecteer **TOTP** om de instellingen vervolgens op te slaan.



The screenshot shows the MFA configuration page. It has a section for 'MFA' with an 'Enable MFA' toggle switch turned on. Below it, the 'Allowed MFA Method' is set to 'TOTP' in a dropdown menu. There is a 'TOTP' section with a note: 'Note: Continue TOTP settings on Pop-up page after clicking Apply.'

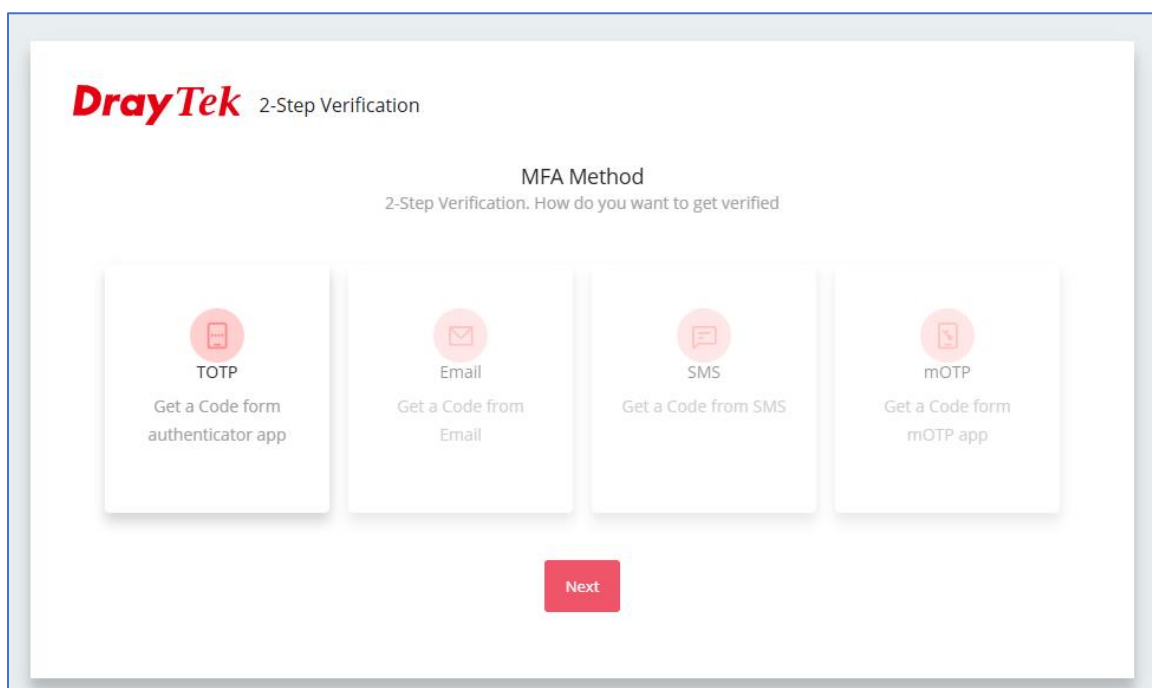
TOTP verificatie

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.



The screenshot shows a window titled "TOTP" with a close button (X) in the top right corner. Inside the window, the text "Secret: TOTP secret" is displayed. Below this is a large QR code labeled "QR Code:". Underneath the QR code is a text input field labeled "Validation Code:". At the bottom right of the window, there are three buttons: "Close", "Skip", and "Apply".

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




The screenshot shows a screen titled "DrayTek 2-Step Verification". Below the title, it says "MFA Method" and "2-Step Verification. How do you want to get verified". There are four selection cards arranged horizontally:

- TOTP**: Get a Code form authenticator app
- Email**: Get a Code from Email
- SMS**: Get a Code from SMS
- mOTP**: Get a Code form mOTP app

At the bottom center of the screen, there is a red "Next" button.

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

DrayTek 2-Step Verification



TOTP 2FA setup

Provide the 6 digit code form the Authenticator app

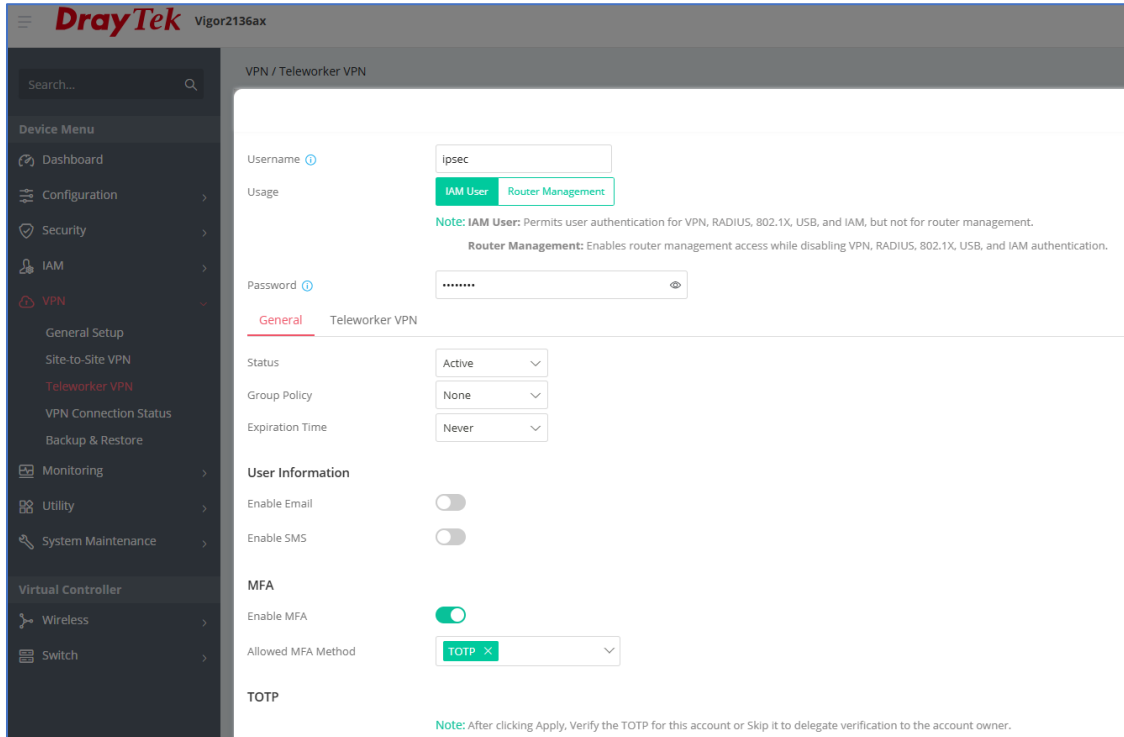
Verify

Try different [authentication](#)

[← Back](#)

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.



The screenshot shows the DrayTek Vigor2136ax web interface. The left sidebar contains a navigation menu with options like Dashboard, Configuration, Security, IAM, VPN, Monitoring, Utility, System Maintenance, Virtual Controller, Wireless, and Switch. The main content area is titled 'VPN / Teleworker VPN' and shows the configuration for a user named 'ipsec'. The 'Usage' section has 'IAM User' selected. The 'Password' field is masked. The 'General' tab is active, showing 'Status' as 'Active', 'Group Policy' as 'None', and 'Expiration Time' as 'Never'. Under 'User Information', 'Enable Email' and 'Enable SMS' are disabled. Under 'MFA', 'Enable MFA' is enabled, and 'Allowed MFA Method' is set to 'TOTP'. A note at the bottom states: 'Note: After clicking Apply, Verify the TOTP for this account or Skip it to delegate verification to the account owner.'


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.



The screenshot shows a dialog box titled 'TOTP'. It contains the following information: 'Secret: TOTP secret', a QR code labeled 'QR Code:', and a 'Validation Code:' input field. At the bottom right, there are three buttons: 'Close', 'Skip', and 'Apply'.

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.

DrayTek 2-Step Verification



TOTP 2FA setup

Provide the 6 digit code form the Authenticator app

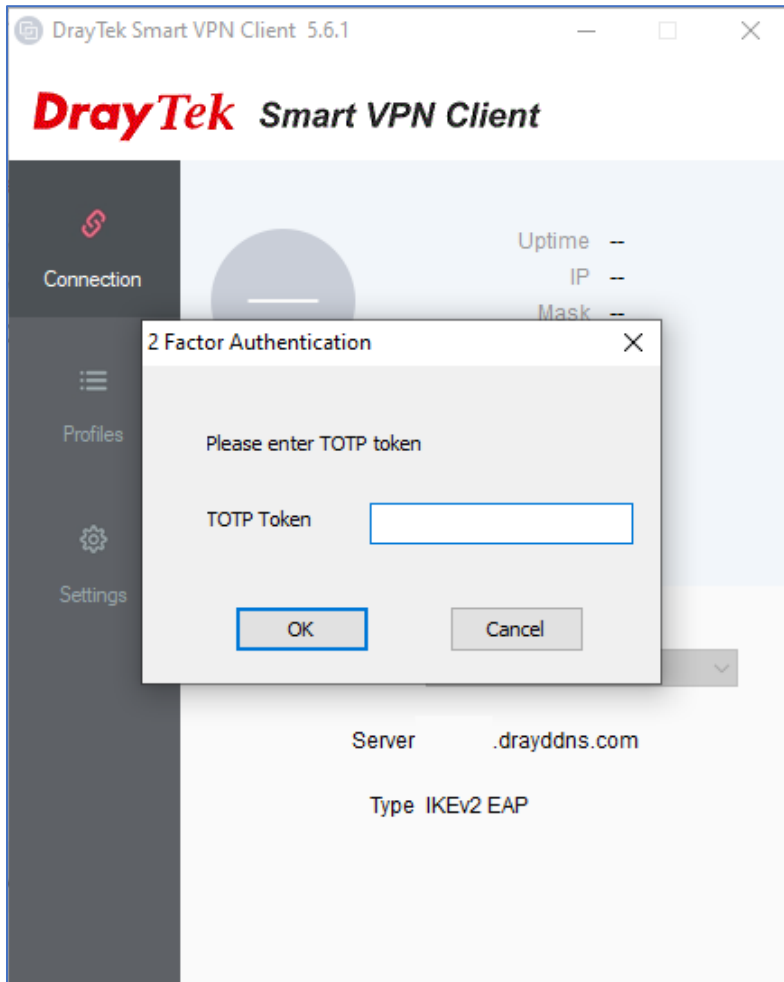
Verify

Try different [authentication](#)

[← Back](#)

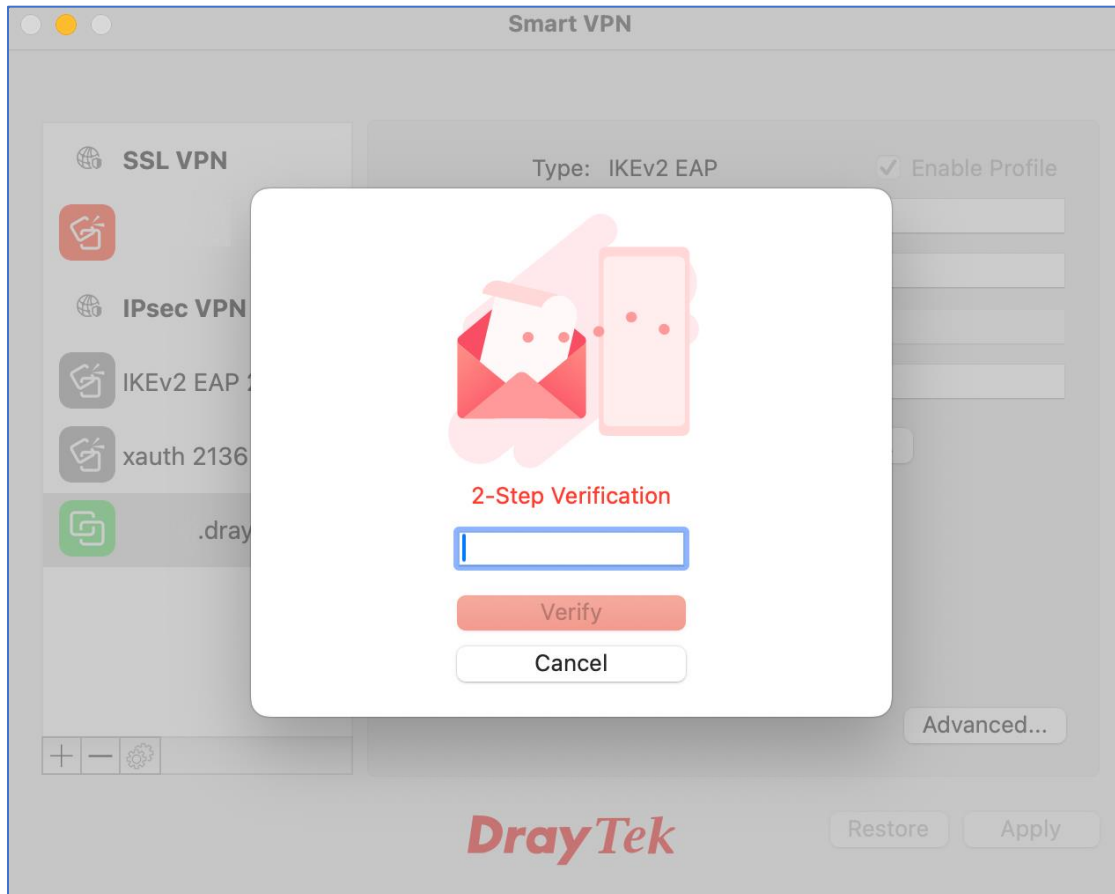
MFA via Smart VPN Client (Windows)

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.

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.