



Handleiding

Twee-staps-authenticatie

In deze handleiding vind je de stappen die je volgt bij:

- Het instellen van de twee-staps-authenticatie
- Het inloggen met de twee-staps-authenticatie
- Het (eventueel) later instellen van de twee-staps-authenticatie





Instellen van twee-staps-authenticatie

Na het inloggen op je e-healthplatform ontvang je vanaf 1 april een notificatie met daarin een introductie van twee-staps-authenticatie. Zolang het optioneel is (van 1 april tót 1 juli), krijg je een uitleg met de keuze om het wel of niet in te stellen. Na 1 juli is het verplicht om middels twee-staps-authenticatie in te loggen.

Introductie van twee-staps-authenticatie

Twee-staps-authenticatie biedt een extra beveiligingslaag voor jouw account. Zo heb alleen jij toegang tot je account, zelfs wanneer iemand achter je wachtwoord is gekomen. Instellen duurt maar één minuut.

Hoe werkt het?

Na het inloggen met je e-mailadres en wachtwoord word je om een authenticatie-code gevraagd. Deze wordt via SMS verstuurd of aangemaakt in een authenticatie-applicatie op je mobiele telefoon.

Waarom is dit veiliger?

Omdat alleen jij toegang tot je mobiele telefoon hebt, kan iemand die achter je wachtwoord is gekomen nog steeds niet bij je account. Met andere woorden, om bij je account te komen heb je niet alleen iets nodig wat alleen jij weet (je wachtwoord), maar ook iets wat alleen jij hebt (je mobiele telefoon).

Moet ik dat iedere keer gebruiken?

Om niet bij iedere keer dat je wilt inloggen je mobiele telefoon nodig te hebben, kun je instellen dat je 1 dag, 3 dagen of een week onthouden wilt worden op dat apparaat. Op deze manier ben je nog steeds beveiligd, want wanneer iemand op een andere apparaat probeert in te loggen met jouw gegevens moeten ze nog steeds een authenticatie-code invullen.

Als je het niet nu wilt instellen, kun je twee-staps-authenticatie altijd onder je instellingen terugvinden.

[Twee-staps-authenticatie instellen](#) [Niet nu](#)



Als je ervoor kiest om twee-staps-authenticatie in te stellen dan volgen er een aantal stappen op de volgende pagina.



1. Je voert nogmaals je wachtwoord in.
2. Er wordt gevraagd of je wilt authenticeren via SMS of via een authenticatie applicatie op je telefoon. In verband met bijkomende kosten bij gebruik van de optie 'SMS met code', verzoeken we om gebruik te maken van een authenticatie applicatie op je telefoon. Een authenticator app genereert telkens automatisch een nieuwe code waarmee je kan inloggen.

Twee-staps-authenticatie inschakelen

Twee-staps-authenticatie biedt een extra beveiligingslaag voor jouw account. Na het inloggen word je om een authenticatie-code gevraagd. Deze ontvang je naar keuze: per SMS of in een authenticatie-applicatie op je mobiele telefoon.

1. Vul je wachtwoord in

2. Kies hoe je authenticatie-codes wilt ontvangen

SMS met code

Ontvang een gratis tekstbericht met authenticatie-code op je mobiele telefoon. Hiervoor is je mobiele telefoonnummer nodig.

Code van authenticatie-applicatie

Gebruik een gratis authenticatie-applicatie die je op je mobiele telefoon moet installeren om authenticatie-codes mee aan te maken.

Doorgaan

Twee-staps-authenticatie niet nu instellen

3. Als je nog geen authenticatie applicatie op je mobiele telefoon hebt, kan je bijvoorbeeld een van onderstaande apps downloaden. De keuze voor welke app is vrij:
 - Microsoft Authenticator (Android, iOS, Windows Phone)
 - Google Authenticator (Android, iOS)
 - LastPass Authenticator (Android, iOS, Windows Phone)
 - 3.1. Om de Authenticator applicatie te downloaden, ga naar:
 - Indien je een Android telefoon hebt: Play Store.
 - Indien je een iPhone hebt: App Store.
 - Indien je een Windows Phone hebt: Windows Phone Store.
 - 3.2. Vul in het zoekveld één van bovenstaand genoemde applicaties in.
 - 3.3. Selecteer de betreffende applicatie en klik vervolgens op 'Download' of 'Installeren'.
4. Na het downloaden van een authenticatie applicatie, scan je de QR-code met je authenticatie app op je mobiele telefoon.

Ontvang een gratis tekstbericht met authenticatie-code op je mobiele telefoon. Hiervoor is je mobiele telefoonnummer nodig.

Code van authenticatie-applicatie

Gebruik een gratis authenticatie-applicatie die je op je mobiele telefoon moet installeren om authenticatie-codes mee aan te maken.

3. Scan deze QR-code met de authenticatie-applicatie op je mobiele telefoon



Als je nog geen authenticatie-applicatie op je mobiele telefoon hebt kun je bijvoorbeeld een van deze downloaden:

- Microsoft Authenticator (Android, iOS, Windows Phone)
- Google Authenticator (Android, iOS)
- LastPass Authenticator (Android, iOS, Windows Phone)

Doorgaan

Twee-staps-authenticatie niet nu instellen



5. Vervolgens vul je de ontvangen code in van je authenticatie applicatie. Elke 30 seconde genereert de app een nieuwe code. De vorige code blijft hierna nog 30 secondes lang geldig; elke code is in totaal dus een minuut geldig.

Als je nog geen authenticatie-applicatie op je mobiele telefoon hebt kun je bijvoorbeeld een van deze downloaden:

- Microsoft Authenticator (Android, iOS, Windows Phone)
- Google Authenticator (Android, iOS)
- LastPass Authenticator (Android, iOS, Windows Phone)

4. Vul de code in van de authenticatie-applicatie

799012

Twee-staps-authenticatie is nu ingeschakeld voor jouw account.

5. Bewaar je herstelcodes op een veilige manier

Wanneer je geen authenticatie-codes kunt ontvangen, bijvoorbeeld wanneer je je mobiele telefoon kwijt bent of deze gestolen is, kun je een herstelcode gebruiken om alsnog toegang te krijgen tot je account. Herstelcodes kunnen slechts eenmalig gebruikt worden. Schrijf je herstelcodes op, print ze uit, of gebruik een wachtwoordmanager zoals 1Password of LastPass om ze op een veilige manier op te slaan.

2E7G-XZX8-C8MW
LS7P-9X7D-SH4V

6RY9-653J-GXPU
QJK4-Y85C-V29E

7JQH-ASUK-M93J
W7UX-5G6Y-TL23

Gedaan

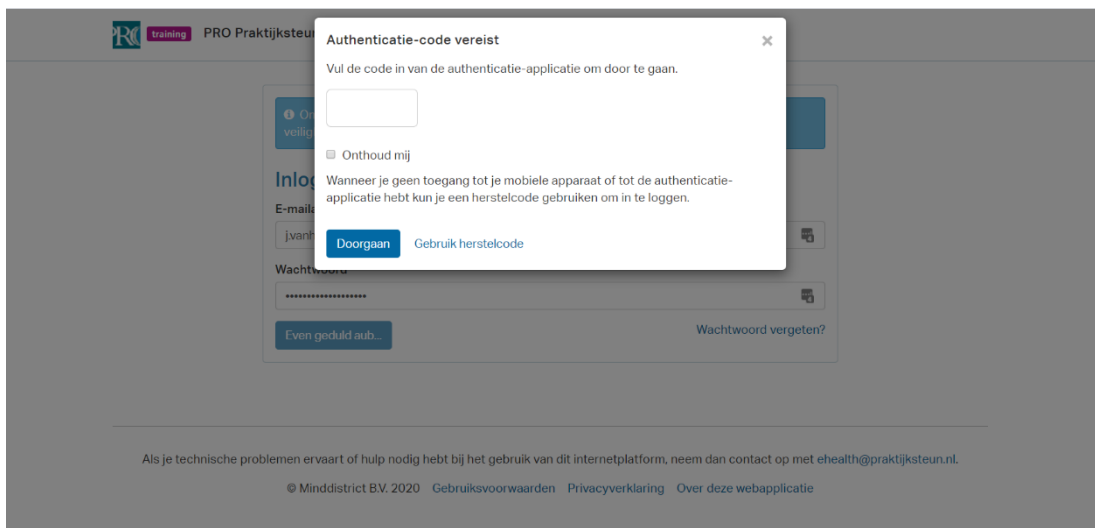
6. Je ontvangt zogenoemde recovery codes om op te slaan op een veilige plek. Deze recovery codes kan je gebruiken om alsnog toegang te krijgen tot je account mocht je bijvoorbeeld je telefoon kwijtraken. Sla de codes daarom goed op.

7. Na het doorlopen van de stappen ben je ingelogd en kun je aan de slag.



Inloggen met twee-staps authenticatie

1. Wanneer je op een ander moment weer gaat inloggen dan word je, na het invoeren van het wachtwoord, gevraagd naar de authenticatie code.
2. Je ontvangt als gebruiker deze code op de authenticatie app die je eerder hebt gebruikt om twee-staps-authenticatie in te stellen.
3. Pas na het invullen van deze code kun je daadwerkelijk inloggen.



4. Wanneer je het vinkje 'Onthoud mij' selecteert, wordt er op het apparaat waar je op dat moment op werkt gedurende 12 uur niet om een authenticatie code gevraagd. Deze wordt dan voor je onthouden.



Twee-staps-authenticatie op een later moment instellen?

Indien je besluit op een later moment de twee-staps-authenticatie in te stellen (dit moet uiterlijk 30 juni ingesteld zijn), kan je dat via de instellingen in je profiel doen:

1. Klik in het e-healthplatform waarin je werkt rechtsboven op je naam.
2. Klik vervolgens op 'Instellingen'.
3. Klik dan op de tegel 'Twee-staps-authenticatie'
4. Klik op 'Twee-staps-authenticatie inschakelen'
5. Vervolgens kan je de eerder genoemde stappen in deze handleiding doorlopen om de twee-staps-authenticatie in te schakelen.

The screenshot shows the user profile page for Judith van Haare in the PRO Praktijksteun Trainingsomgeving. The navigation bar includes Home, Catalogus, Taken (3), Gesprekken, Cliënten, Professionals (selected), Data, and Configuratie. The profile section shows a circular profile picture placeholder with a camera icon, the name Judith van Haare, and a menu with options: Details, Instellingen (selected), and Caseload. The main heading is 'Twee-staps-authenticatie'. Below it, the text reads: 'Twee-staps-authenticatie biedt een extra beveiligingslaag voor jouw account. Na het inloggen word je om een authenticatie-code gevraagd. Deze ontvang je naar keuze: per SMS of in een authenticatie-applicatie op je mobiele telefoon.' Below this, it states 'Twee-staps-authenticatie is uitgeschakeld.' and there is a blue button labeled 'Twee-staps-authenticatie inschakelen'.



Vragen?

Voor vragen over het gebruik van videobellen kan je terecht bij de helpdesk. De contactgegevens van de helpdesk staan onderaan de pagina op elk e-healthplatform vermeld.