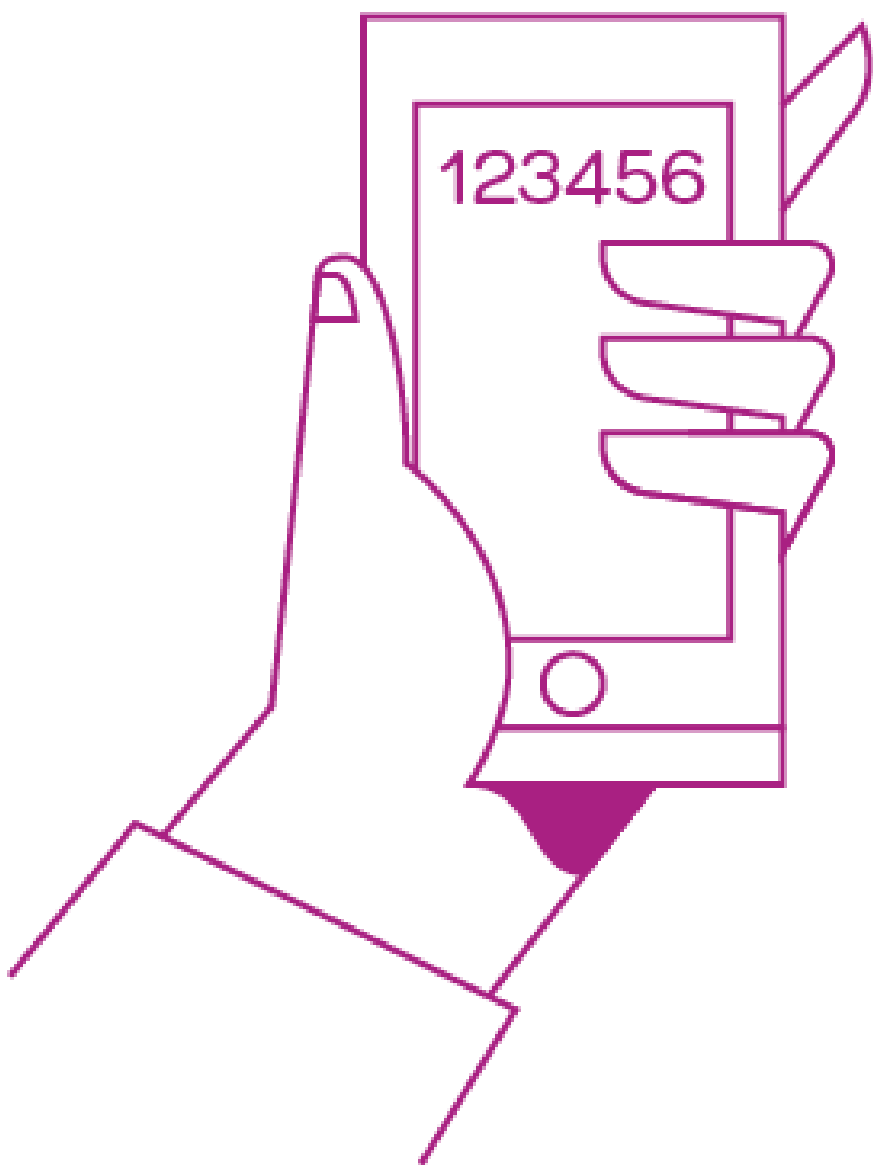


Twee-staps-authenticatie implementeren



minddistrict



Minddistrict nog veiliger
met twee-staps-
authenticatie

Dit document bevat een uitgebreide instructie om twee-staps authenticatie (2FA) te implementeren.

Twee-staps authenticatie is een aanvullende functionaliteit waarvoor aanvullende kosten in rekening worden gebracht. Wil je meer informatie? Neem contact op met je accountmanager.

Inhoud

<u>WAT IS TWEE-STAPS AUTHENTICATIE?</u>	<u>3</u>
<u>HOE WERKT TWEE-STAPS AUTHENTICATIE?</u>	<u>3</u>
TWEE-STAPS AUTHENTICATIE INSTELLEN	3
INLOGGEN MET TWEE-STAPS AUTHENTICATIE	4
WANNEER WORDT ER OM EEN AUTHENTICATIECODE GEVRAAGD?	5
JE GEBRUIKERSINSTELLINGEN AANPASSEN	5
<u>TWEE-STAPS AUTHENTICATIE CONFIGUREREN OP JE PLATFORM</u>	<u>6</u>
DOOR WIE IS TWEE-STAPS AUTHENTICATIE IN TE RICHTEN?	6
WELKE CONFIGURATIEMOGELIJKHEDEN ZIJN ER?	6
<u>BIJZONDERE SITUATIES</u>	<u>7</u>
WAT ALS IEMAND ZIJN MOBIELE TELEFOON KWIJTRAAKT?	7
WAT ALS IK AL MIJN RECOVERY CODES GEBRUIKT HEB OF ZE KWIJT BEN?	7
<u>AANDACHTSPUNTEN BIJ IMPLEMENTATIE</u>	<u>7</u>

Wat is twee-staps authenticatie?

Twee-staps authenticatie (2FA) biedt een extra beveiligingslaag voor gebruikersaccounts. Na het inloggen met e-mailadres en wachtwoord moet tevens een authenticatiecode worden ingevoerd die via SMS verstuurd wordt of met een authenticatie-applicatie op de mobiele telefoon gegenereerd kan worden.

Hoe werkt twee-staps authenticatie?

Twee-staps authenticatie instellen

De stap voor de gebruiker om twee-staps authenticatie in te stellen volgt nadat je je wachtwoord hebt aangemaakt en akkoord bent met de gebruiksvoorwaarden. Als het zo is ingericht dat 2FA optioneel is dan krijg je een uitleg met de keuze om het wel of niet in te stellen.



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 de gebruiker ervoor kiest om Twee-staps-authenticatie in te stellen dan volgen er aan aantal stappen op de volgende pagina:

1. Je voert nogmaals je wachtwoord in
2. Kies of je wilt authenticeren via SMS (a) of een authenticatie applicatie op je telefoon (b)

3. Je vult je telefoonnummer in (a) of je scant de QR code met je authenticatie applicatie (b)
4. Je vult de ontvangen code in.
5. Je ontvangt je recovery codes om op te slaan op een veilige plek.



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 wordt via SMS verstuurd of aangemaakt 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.

3. Vul je mobiele telefoonnummer in waarop je authenticatie-codes via SMS wilt ontvangen

0612345678

Dit mobiele telefoonnummer wordt alleen gebruikt voor twee-staps-authenticatie. Wanneer je een nieuw mobiele telefoonnummer krijgt kun je de instellingen voor twee-staps-authenticatie aanpassen.

4. Vul de code in van de SMS die je ontvangen hebt

014784

[Twee-staps-authenticatie inschakelen](#)

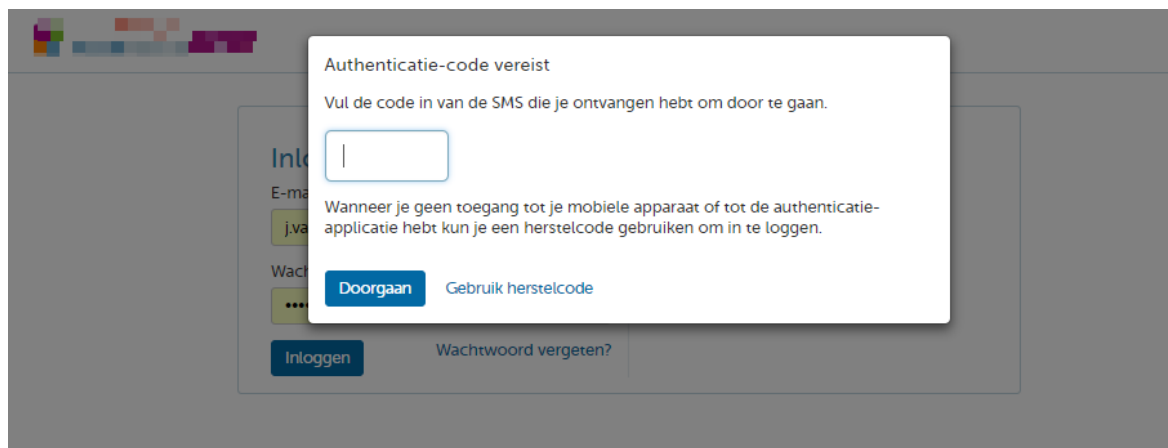
[SMS opnieuw versturen](#)

[Mobiele telefoonnummer aanpassen](#)

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

Inloggen met twee-staps authenticatie

Wanneer je op een ander moment weer gaat inloggen dan wordt je - na het invoeren van je wachtwoord - gevraagd naar de authenticatie code. Je ontvangt als gebruiker deze code op het telefoonnummer/authenticatie app die je eerder hebt gebruik om 2FA in te stellen. Pas na het invullen van deze code kun je daadwerkelijk inloggen.



Wanneer wordt er om een authenticatiecode gevraagd?

Indien 2FA is ingesteld, wordt op verschillende momenten om een authenticatiecode gevraagd:

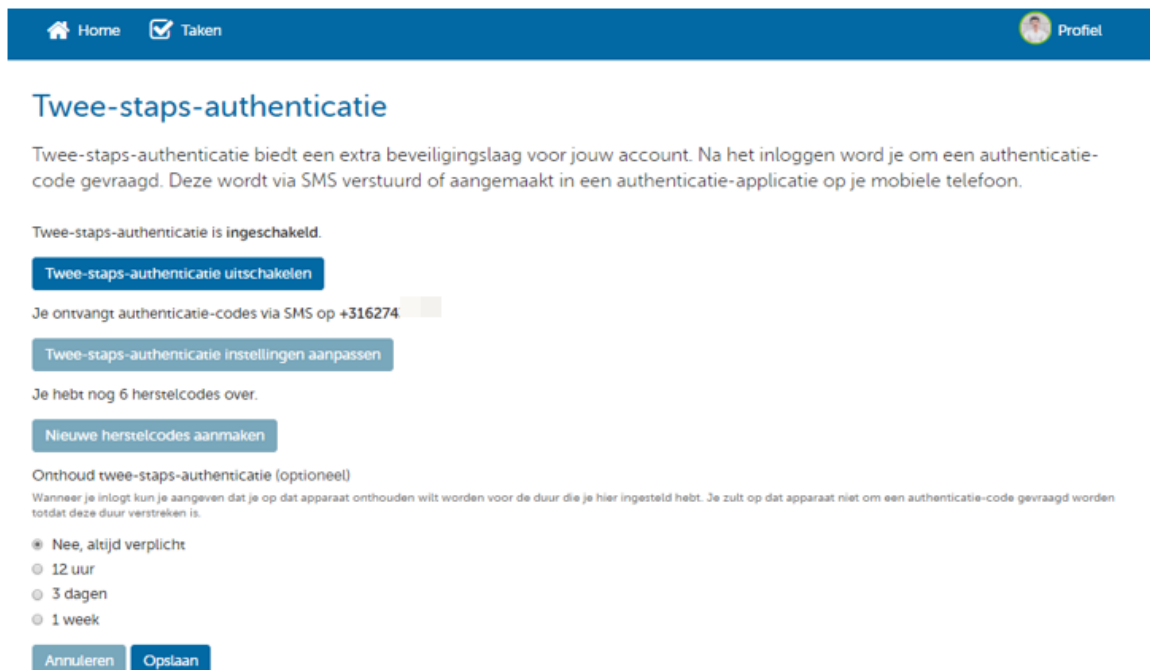
- Bij het inloggen
- Bij het veranderen van het wachtwoord
- Bij gebruik van 'wachtwoord vergeten'
- Na één uur inactiviteit
- Bij het uitzetten van 2FA

Daarnaast wordt om het wachtwoord gevraagd bij:

- Veranderen 2FA instelling
- Aanvragen nieuwe recovery codes
- Uitzetten 2FA

Je gebruikersinstellingen aanpassen

Je kunt als gebruiker je twee-staps authenticatie aanpassen via de instellingen in je profiel.



The screenshot shows a user profile page with a blue header containing 'Home', 'Taken', and 'Profiel'. The main heading is 'Twee-staps-authenticatie'. Below it, a paragraph explains that two-step authentication provides an extra security layer and is triggered via SMS or an app. A status message indicates it is 'ingeschakeld' (turned on). There are three buttons: 'Twee-staps-authenticatie uitschakelen', 'Twee-staps-authenticatie instellingen aanpassen', and 'Nieuwe herstelcodes aanmaken'. The 'instellingen aanpassen' button is highlighted. Below, a section titled 'Onthoud twee-staps-authenticatie (optioneel)' allows users to specify a duration for which the device is trusted. The 'Nee, altijd verplicht' option is selected. Other options are '12 uur', '3 dagen', and '1 week'. At the bottom are 'Annuleren' and 'Opslaan' buttons.

Instellingen wijzigen als cliënt



Mieke de Graaff

- Details
- Instellingen
- Caseload

Twee-staps-authenticatie

Twee-staps-authenticatie biedt een extra beveiligingslaag voor jouw account. Na het inloggen word je om een authenticatie-code gevraagd. Deze wordt via SMS verstuurd of aangemaakt in een authenticatie-applicatie op je mobiele telefoon.

Twee-staps-authenticatie is **ingeschakeld**.

Je ontvangt authenticatie-codes via SMS op +316274-

Twee-staps-authenticatie instellingen aanpassen

Je hebt nog 6 herstelcodes over.

Nieuwe herstelcodes aanmaken

Annuleren

Instellingen wijzigen als professional

Twee-staps authenticatie configureren op je platform

Door wie is twee-staps authenticatie in te richten?

De functionaliteit kan door een gebruiker met de rol 'applicatiebeheerder' ingericht worden. Dit doe je bij het menu 'Configuratie' bij 'Web-authenticatie'.

Let op: twee-staps authenticatie is niet als standaard functionaliteit beschikbaar. Deze functie kan pas door de applicatiebeheerder worden geconfigureerd zodra deze door Minddistrict beschikbaar is gesteld op je platform.

Welke configuratiemogelijkheden zijn er?

Een applicatiebeheerder heeft voor professionals de volgende opties:

- **Uit** (2FA staat uit)
- **Optioneel** (een professional kán 2FA instellen)
- **Verplicht** (een professional moet 2FA instellen zodra hij inlogt)

Bovendien kan de applicatiebeheerder instellen of en hoe lang de authenticatiecode onthouden mag worden op een specifiek apparaat. Hij kan kiezen uit:

- Nee, niet onthouden
- 12 uur
- 3 dagen
- 1 week

Voor cliënten en naasten heb je de volgende keuze-opties:

- **Uit** (2FA staat uit)
- **Optioneel** (een cliënt/naaste kán 2FA instellen)

Cliënten en naasten mogen zelf bepalen hoe lang hun code onthouden wordt op een specifiek apparaat.

Bijzondere situaties

Wat als iemand zijn mobiele telefoon kwijtraakt?

Bij het instellen van 2FA ontvangt de gebruiker 6 recovery codes die eenmalig gebruikt kunnen worden wanneer de gebruiker geen toegang heeft tot authenticatiecodes, bijvoorbeeld wanneer de mobiele telefoon kwijt of gestolen is. Met deze recovery codes kan de gebruiker alsnog toegang krijgen tot zijn account.

Wanneer een gebruiker óók de recovery codes kwijt is, dient hij contact op te nemen met iemand die 2FA voor zijn account kan resetten.

- Een applicatiebeheerder kan 2FA resetten voor **professionals**
- Een gekoppelde professional en een secretaresse kan 2FA resetten voor een **cliënt**
- Op dit moment kan niemand 2FA resetten voor naasten, omdat er geen professional aan een naaste gekoppeld is, en secretaresses geen naasten zien.

Wanneer 2FA is ingesteld op 'verplicht', kan een applicatiebeheerder 2FA ook tijdelijk (1 maand) uitzetten voor een professional, in geval er geen mobiele telefoon beschikbaar is om 2FA op in te stellen. Dit doe je via het profiel van een professional.

Wat als ik al mijn recovery codes gebruikt heb of ze kwijt ben?

Een gebruiker kan op ieder moment nieuwe recovery codes aanvragen. Hiermee vervallen de oude recovery codes.

Aandachtspunten bij implementatie

Het implementeren van twee-staps authenticatie vergt zorgvuldigheid. Inloggen is voor veel gebruikers vaak al lastig zonder deze tweede beveiligingslaag. Laat staan als er dus nog een drempel bij komt. Denk bij de implementatie na over het volgende:

- Test de configuratie-instellingen heel goed door op een trainingsomgeving.
- Zorg dat hulpverleners op de hoogte zijn.
 - Hoe werkt het voor hun?
 - Hoe werkt het voor cliënten?

- Hoe resetten zij de authenticatie voor hun cliënt in het geval hij zijn mobiele telefoon kwijt is?
- Zorg dat secretariaten op de hoogte zijn.
 - Hoe werkt het voor hun?
 - Hoe werkt het voor cliënten?
 - Hoe resetten zij de authenticatie voor hun cliënt in het geval hij zijn mobiele telefoon kwijt is?
- Zorg dat alle applicatiebeheerders en andere ondersteunende functies (zoals interne helpdesk) weten hoe 2FA authenticatie werkt.
 - Hoe werkt het voor hun?
 - Hoe werkt het voor professionals?
 - Hoe werkt het voor cliënten?
 - Hoe resetten zij de authenticatie voor een gebruiker in het geval hij zijn mobiele telefoon kwijt is?

