

HANDLEIDING 2-STAPS VERIFICATIE

Verantwoordelijke uitgever (v.u.): Siegelinde Lacoere | Algemeen Directeur Stad Oostende | Vindictivelaan 1, 81400 Oostende

Uit PAS
Middenkust

Beveilig je account met 2-staps verificatie om aan te melden op de UiTPAS balie

Als gebruiker van de UiTPAS balie-applicatie verwerk je persoonsgegevens die zorgvuldig behandeld moeten worden. Daarom vullen we onze beveiligingsmaatregelen regelmatig aan. De volgende stap die we daarin nemen is de invoering van 2-staps verificatie.

Wat is 2-staps verificatie

Twee-staps verificatie betekent dat je bij het aanmelden naast je emailadres en wachtwoord ook een extra code zal moeten invoeren als extra beveiligingsstap. Je kan kiezen om die code te ontvangen **via een app of via een SMS**.

Hoe beveilig je jouw account via een app of via een SMS?

- Surf naar de balie-applicatie
- Op het aanmeldscherm klik je onderaan op **“Beveilig nu al je account met 2-stapsverificatie”** en doorloop de verschillende stappen.
- Je meldt vanaf dan aan in de balie met extra beveiliging

Op deze website vind je de stap-voor-stap uitleg

Hoe kan je de 2-staps verificatie instellen in je webbrowser?

We begrijpen dat niet alle baliemedewerkers een werktelefoon of altijd een persoonlijke smartphone bij de hand hebben. Het instellen van 2-stapsverificatie via een webbrowser kan hier een oplossing bieden.

Stap 1: haal een QR-code op uit de balie-applicatie

- Open de UiTPAS-beheersapplicatie (versie 25.03.035).
- Klik op 'beveilig je account met 2-staps verificatie'
- Meld je aan met je UiTID (je werk-mailadres)
- Noteer de verificatiecode (6 cijfers) die je per mail ontvangt
- Kies 'Verder met de authenticator app'
- Maak een schermafbeelding van de QR-code en sla deze veilig op op je computer. Zorg dat alleen de QR-code zichtbaar is.

The image shows two screenshots of the UiTID application interface. The left screenshot is titled 'stap 2/3' and '2-stapsverificatie instellen'. It instructs the user to choose how to secure their UiTID: either with an authenticator app (recommended) or via SMS. Under 'Code via authenticator app', it lists Google Authenticator, Microsoft Authenticator, and Authy as examples. A blue button labeled 'Verder met authenticator app' is visible. Below it is a link 'Hulp nodig met authenticator?'. The 'Code via SMS' section mentions that if the user doesn't have a smartphone, they can choose SMS verification. A blue button labeled 'Verder met SMS' is also present. The right screenshot is titled 'stap 3/3' and 'Code via authenticator app'. It instructs the user to open their authenticator app and scan the QR code. A QR code is displayed in the center. Below it is a text input field for the 'Verificatiecode (6 cijfers)'. A blue button labeled 'Ga verder' is at the bottom. To the right of this input field is another QR code. A link 'Hulp nodig met authenticator?' is also present.

Stap 2: Authenticator-extensie installeren en instellen

Belangrijk: Zorg dat je stap 1 hebt afgerond (QR-code opgeslagen), anders kun je niet verder.

- **Installeer de extensie**
 - Microsoft Edge: ga naar Authenticator: 2FA Client – Microsoft Edge Addons en installeer de extensie of via [Authenticator: 2FA Client – Microsoft Edge Addons](#)
 - Google Chrome: Ga naar Authenticator – Chrome Web Store en installeer de extensie of via [Authenticator – Chrome Web Store](#)

- **Open de extensie**

- Klik op het puzzelstukje rechtsboven in je browser 
- Klik op het pinnetje om de extensie vast te zetten in je werkbalk 
- Selecteer **Authenticator: 2FA Client** bij Microsoft Edge of **Authenticator** bij Google Chrome

- **Voeg je account toe**

- Open de Authenticator-extensie
- Klik op **bewerken** (potloodje rechtsboven) 
- Klik op het **plusje** om een account toe te voegen 
- Kies **QR-afbeelding importeren**
- Upload de QR-code die je in stap 1 hebt opgeslagen via **QR-afbeeldingsback-up importeren**

QR-afbeeldingsback-up importeren

- **Klaar!**

- Open opnieuw de balieapplicatie om je registratie af te ronden. Vanaf nu kun je de code uit de Authenticator-extensie gebruiken om veilig in te loggen.

Extra aandachtspunten

- Meld je momenteel aan met een “algemeen emailadres” zoals “info@”? Zet deze dan om naar een individuele account op naam, gezien je account nu met de 2de stap gelinkt is aan je persoonlijke smartphone en/of je gsm-nummer.
- Je kan kiezen om de code te ontvangen via een app en/of SMS. We raden aan om, indien mogelijk, beide methoden in te stellen. Wanneer je bv. de SMS niet meteen ontvangt, kan je alsnog de code in de app ophalen.

Veelgestelde Vragen

Heb ik een smartphone nodig?

Nee, je hebt geen smartphone nodig.

Indien je niet beschikt over een smartphone kan je kiezen om de code enkel te ontvangen via SMS.

Kan de code niet via email verstuurd worden?

Nee, om veiligheidsredenen kan je de code niet via email ophalen. De code via app of SMS ophalen is een pak veiliger dan via email. Als iemand toegang heeft tot je mailbox, kan die namelijk ook je aanmeldcodes onderscheppen en zo in je account geraken. Via sms of een authenticator-app blijft die tweede stap echt gescheiden, een extra beschermingslaag dus voor je account.

Ik wil graag met een code via de app werken. Hoe doe ik dat?

In dit artikel vind je stap-voor-stap hoe je de code met een app kan ophalen. Voordeel is dat je dan niet moet wachten op een smsje.

Hoe vaak moet ik de extra code ingeven?

Op hetzelfde toestel moet je om de 7 dagen de extra code ingeven. Op een nieuw toestel of andere browser zal de code opnieuw gevraagd worden.