



Q-interactive®

Handleiding voor gebruik 2-Factor Authentication (2FA)

Q-interactive gebruikershandleiding

Mei 2018



Pearson

2-factor authentication (2FA) is een aanvulling op uw gebruikersnaam en wachtwoord om de beveiliging van uw account(s) op Q-interactive en/of Q-global verder te verhogen. Wanneer u zich aanmeldt via 2FA, voert u zoals gebruikelijk uw gebruikersnaam en wachtwoord in, maar daarnaast ook een eenmalige code die alleen voor u beschikbaar is. Hiermee zijn de gegevens in uw account extra beveiligd.

Pearson heeft 2-Factor Authentication ingevoerd op Q-interactive en Q-global om te voldoen aan de vereisten van de nieuwe privacywetgeving GDPR (Algemene Verordening Gegevensbescherming).

De eerste keer dat u zich aanmeldt bij Q-interactive Central voordat 2FA is geactiveerd, ziet u een venster dat beschrijft wat 2FA is:

Twee-factor Verificatie (2FV)

Wat is twee-factor verificatie en hoe werkt het?

Twee-factor verificatie is een veiligheidsoptie die het Q-interactive account helpt te beschermen in aanvulling op uw gebruikersnaam en wachtwoord. Wanneer u de twee-factor verificatie hebt aangezet, dan zal u gevraagd worden om een aanvullende veiligheidscode in te vullen of uw login-poging te bevestiging, na het succesvol invoeren van uw gebruikersnaam en wachtwoord.

Er zijn verscheidene verificatie methoden* die u kunt gebruiken bij u Q-interactive account voor de twee-factor verificatie:

- Veiligheidscode van Google Verificator
- Tekstbericht (sms) code van uw geregistreerde mobiele telefoon *(hier zijn mogelijk kosten aan verbonden)*
- Email code van uw geregistreerde emailadres

Let op: mogelijk zijn niet alle verificatie methoden beschikbaar voor u, afhankelijk van wat er per land mogelijk is.*

U kunt zoveel aanvullende verificatie methoden toevoegen als u wilt, er moet echter minimaal een toegevoegd zijn om in te loggen in Q-Interactive.

Heb ik elke keer dat ik inlog een twee-factor verificatie nodig?

U zult u elke 12 uur opnieuw moeten authenticeren met de twee-factor verificatie, zelfs als u dezelfde browser en computer gebruikt. Indien u inlogt met een andere browser of op een andere computer, dat dient u opnieuw te authenticeren, zelfs binnen het 12-uur tijdsframe.

Voor de Assess iPad applicatie is het nodig om de eerste keer dat u online inlogt (terwijl u verbonden bent aan het internet) op beide iPads te authenticeren. U krijgt de optie om het apparaat te onthouden, indien u hiervoor kiest dan moet u elke 30 dagen opnieuw authenticeren. Indien u ervoor kiest om dit apparaat niet te onthouden, dan moet u elke 12 uur opnieuw authenticeren op elk apparaat.

Let op -indien Assess gebruikt wordt in de offline modus, dan is het niet nodig om de twee-factor verificatie te gebruiken en kunt u inloggen met uw opgeslagen offline gegevens.

U kunt zoveel aanvullende verificatie methoden toevoegen als u wilt, er moet echter minimaal een toegevoegd zijn om in te loggen in Q-Interactive.

Hoe lang zijn de email/sms codes geldig?

Vul 2FV details in

U kunt niet verder voordat u ten minste één verificatiemethode heeft ingesteld. Op de volgende pagina ziet u de beschikbare methodes voor Q-interactive.

Klik op **Vul 2FV details in** om verder te gaan.

Op de volgende pagina kunt u drie verschillende methoden voor 2FA instellen: Google Authenticator, SMS of e-mail. De eerste is een app die gratis te downloaden is op de meeste smartphones. De app genereert eenmalige codes die kunnen worden gebruikt om in te loggen bij verschillende websites en applicaties. Google Authenticator is gemakkelijk te gebruiken en werkt zonder internet- en netwerkverbinding. De applicatie genereert elke 30 seconden een nieuwe code en is daarom een zeer zekere methode voor 2-Factor Authentication.

Twee-factor Verificatie ?

Opslaan

Mijn profiel

Wachtwoord wijzigen

Twee-factor Verificatie

Pearson NL Site License - spieters

U kunt zoveel aanvullende verificatie methoden gebruiken als u zou willen, u moet er echter MINIMAAL EEN kiezen om in te loggen in Q-Interactive. Sta andere optionele methoden toe, wanneer toepasbaar om verificatie issues te minimaliseren. De gegenereerde codes zullen verstuurd worden naar het opgegeven emailadres of mobiele nummer tijdens deze setup en later wanneer er gevraagd wordt om een login voor de Twee-Factor Verificatie.

Het is nodig om de Google Verificator (GV) op uw mobiele apparaat te downloaden voor het instellen. Met een nieuwe telefoon, moet u [stel Google Verificatie opnieuw in](#).

Google Verificatie Set-up **Stel GV in**

2FV Emailadres **Valideer**

Email code **Bevestigen**

2FV Mobile telefoonnummer **Valideer**

Mobiele telefoon code **Bevestigen**

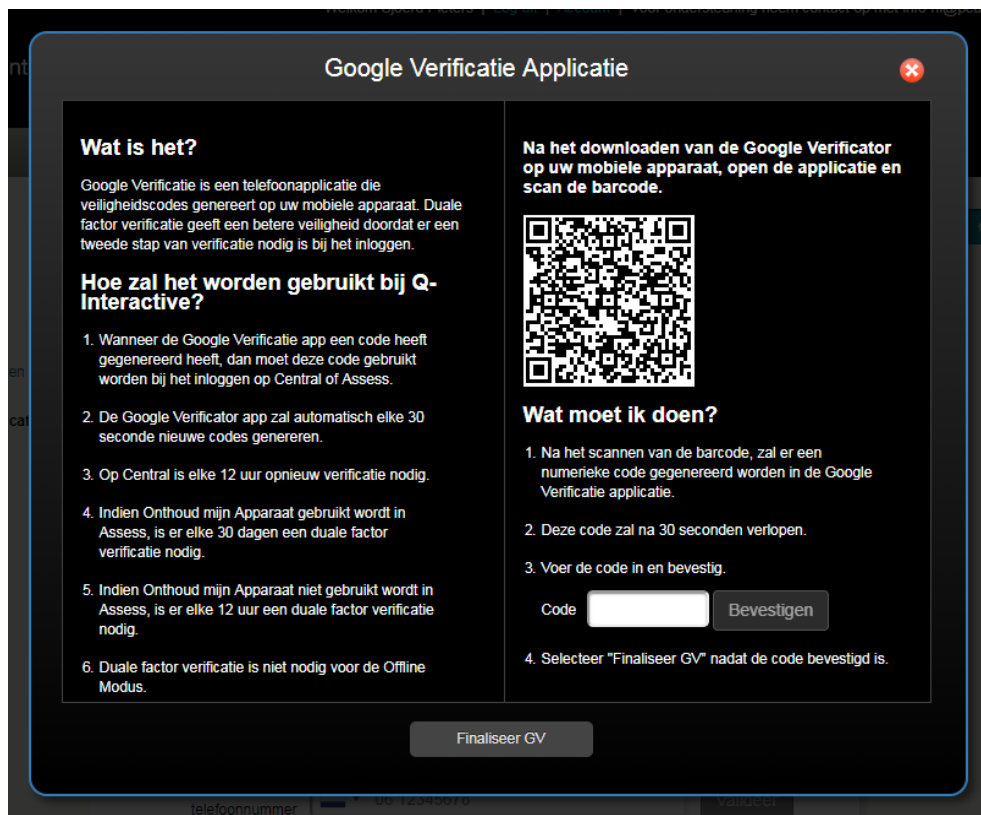
Tips

- Er is slechts een Twee-Factor Verificatie optie nodig.
- De Google Verificatie mobiele applicatie moet gedownload worden voor de set-up.
- Twee-Factor Verificatie email mag niet leeggelaten worden. Moet worden gevalideerd en bevestigd.
- Twee-Factor Verificatie mobiele telefoon mag niet leeggelaten worden. Moet worden gevalideerd en bevestigd.

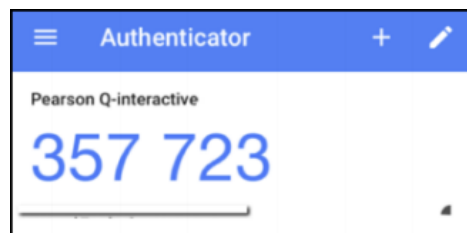
Als u Google Authenticator wilt inschakelen, moet u eerst de app downloaden. Zoek naar "Google Authenticator" in de App Store, Google Play, BlackBerry World of Microsoft Store, afhankelijk van of u een iPhone, Android, BlackBerry of Windows Phone heeft. Zodra Google Authenticator op uw telefoon is geïnstalleerd, opent u de app en klikt u op het plusteken. Kies "Streepjescode scannen" en accepteer dat de app toegang heeft tot de camera van de telefoon.

Klik vervolgens op **Stel GV in** in Central.

Rechtsboven bevindt zich een QR-code die met de mobiele telefoon kan worden gescand.



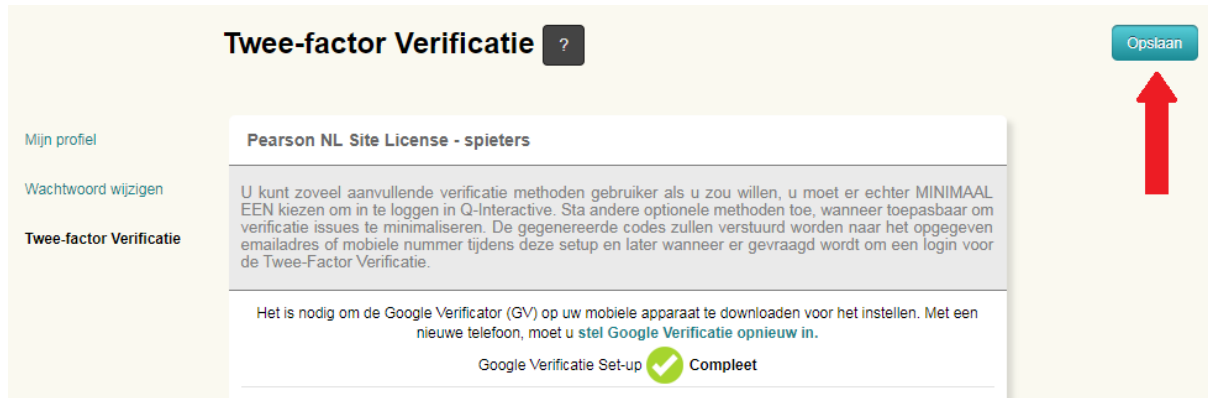
Pak de telefoon op en richt de camera op de QR-code in beeld zodat de QR-code in het vak op de telefoon verschijnt. Een zescijferig nummer wordt weergegeven op de telefoon:



Voer het nummer in (zes cijfers, spatie hoeft niet te worden opgegeven) in punt 3 op Q-interactive Central en klik op **Bevestigen**. Een groen vinkje verschijnt om te bevestigen dat de code is geverifieerd. Klik vervolgens op **Finaliseer GV**.



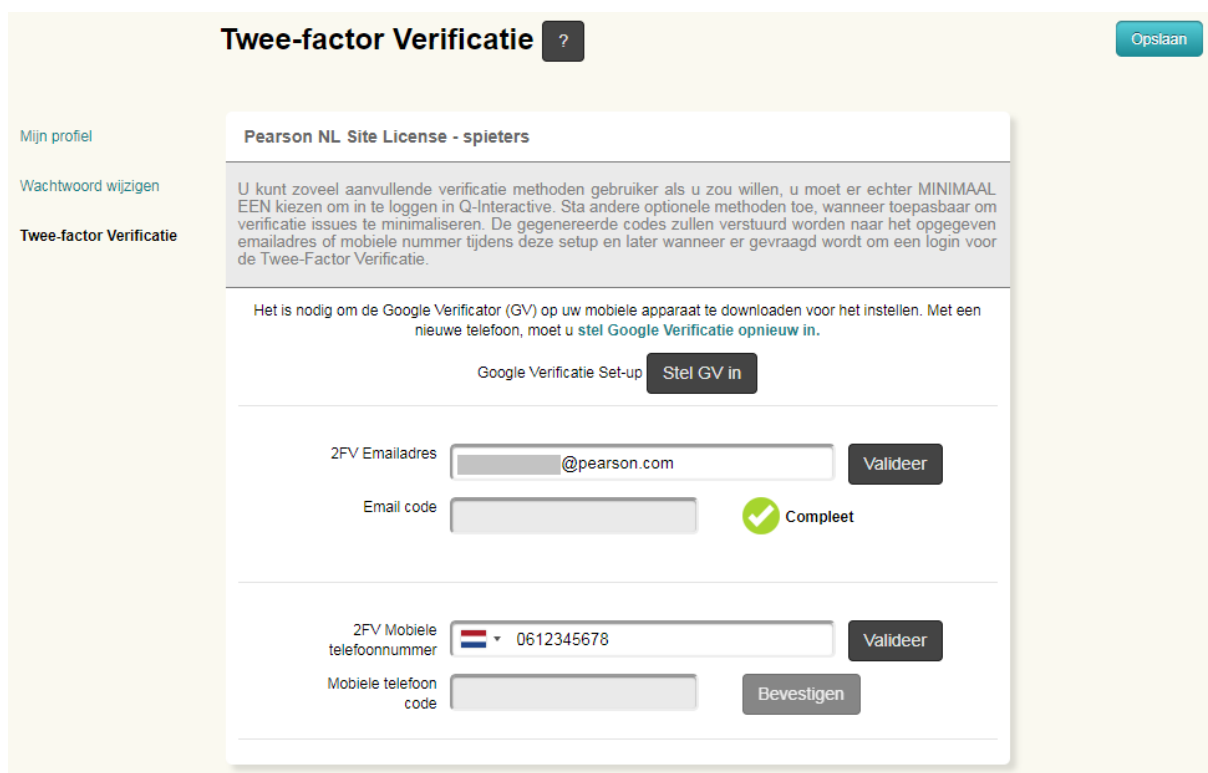
BELANGRIJK: Klik om de authenticatie methode definitief op te slaan en om af te sluiten op **Opslaan** in de rechterbovenhoek.



The screenshot shows the 'Twee-factor Verificatie' page for 'Pearson NL Site License - spieters'. The left sidebar contains links for 'Mijn profiel', 'Wachtwoord wijzigen', and 'Twee-factor Verificatie'. The main content area has a heading 'Pearson NL Site License - spieters' and a paragraph explaining that at least one additional verification method must be chosen. Below this, it states that the Google Authenticator (GV) app needs to be downloaded and installed. A progress indicator shows 'Google Verificatie Set-up' with a green checkmark and the word 'Compleet'. In the top right corner, there is a blue 'Opslaan' button with a red arrow pointing to it.

Google Authenticator is nu ingeschakeld in uw account en u moet vanaf nu een zescijferig nummer, gegenereerd door Google Authenticator, invoeren wanneer u zich aanmeldt bij Q-interactive Central en Assess. 2FA is 12 uur geldig op dezelfde computer.

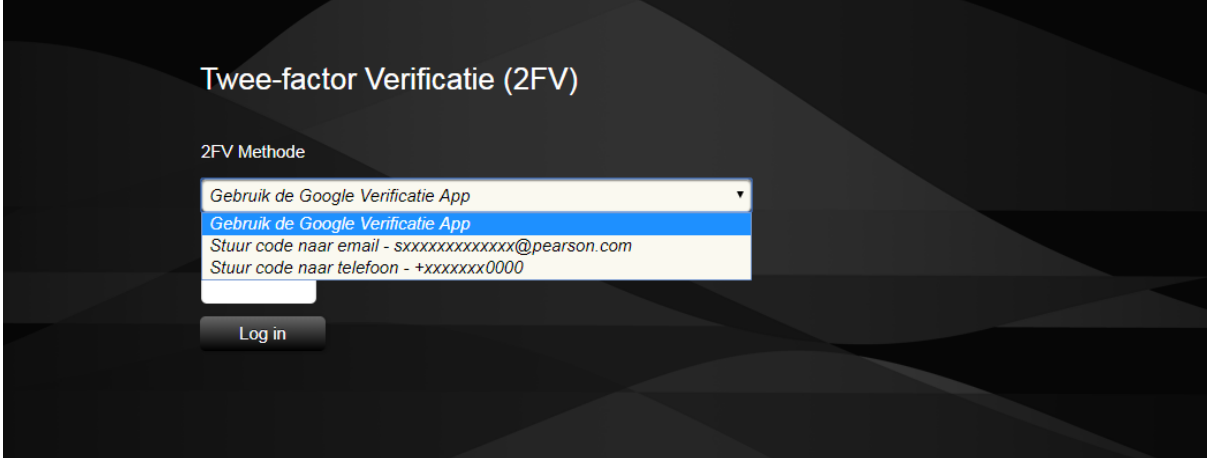
2FA via sms of e-mail wordt op dezelfde manier geconfigureerd.



This screenshot shows the same 'Twee-factor Verificatie' page, but with configuration options for email and mobile phone. The 'Google Verificatie Set-up' button is now 'Stel GV in'. Below, there are two sections: '2FV E-mailadres' with a text input field containing '@pearson.com' and a 'Valideer' button; and '2FV Mobiele telefoonnummer' with a dropdown menu showing a Dutch flag and the number '0612345678', and a 'Valideer' button. Below these are empty input fields for 'Email code' and 'Mobiele telefoon code', with a green checkmark and 'Compleet' next to the 'Email code' field, and a 'Bevestigen' button next to the 'Mobiele telefoon code' field. The 'Opslaan' button remains in the top right corner.

Voer het e-mailadres of mobiele telefoonnummer in en klik op **Valideer**. Er wordt een eenmalige code naar uw e-mailadres of telefoon gestuurd, afhankelijk van de methode die u hebt geselecteerd. Voer de code in het daarvoor bestemde vak in, en klik op **Bevestigen**. Een groene schijf bevestigt dat het configuratieproces is voltooid. Vergeet ook nu niet om in de rechterbovenhoek op **Opslaan** te klikken.

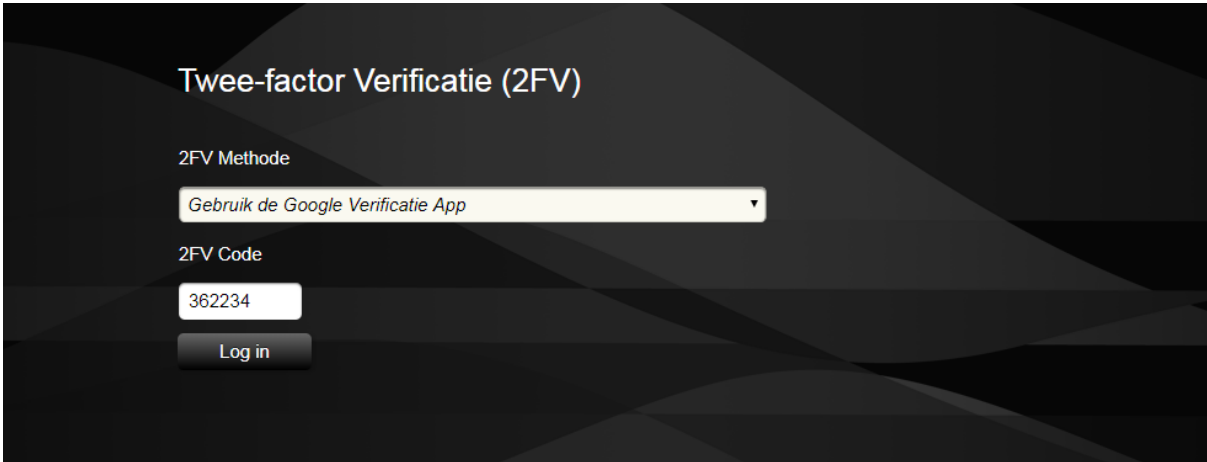
De volgende keer dat u zich aanmeldt, wordt u gevraagd om een 2FA-methode te selecteren. Als u meer dan één verificatiemethode hebt gekozen dan kunt u hiertussen kiezen. Kies er bijvoorbeeld voor de code per e-mail te ontvangen of Google Authenticator te gebruiken.



The screenshot shows a dark-themed login interface titled "Twee-factor Verificatie (2FV)". Below the title, there is a label "2FV Methode" and a dropdown menu. The dropdown menu is open, showing three options: "Gebruik de Google Verificatie App" (highlighted in blue), "Stuur code naar email - sxxxxxxxxxxxxx@pearson.com", and "Stuur code naar telefoon - +xxxxxxxx0000". Below the dropdown menu is a "Log in" button.

Voer de code van Google Authenticator, sms of e-mail in en klik op **Log in**.

Wanneer u zich aanmeldt bij de Assess-app op de iPad van de testleider of cliënt, moet u ook een eenmalige code invoeren, als deze iPads verbonden zijn met internet. Voer uw gebruikersnaam en wachtwoord in zoals gewoonlijk. Selecteer vervolgens de authenticatiemethode en voer de eenmalige code op dezelfde manier in als wanneer u inlogt bij Central.



The screenshot shows the same dark-themed login interface titled "Twee-factor Verificatie (2FV)". Below the title, there is a label "2FV Methode" and a dropdown menu with "Gebruik de Google Verificatie App" selected. Below the dropdown menu is a label "2FV Code" and a text input field containing the code "362234". Below the input field is a "Log in" button.

Als u SMS of e-mail kiest, klikt u op **Verzenden** en voert u de code in die u ontvangt.

Klik vervolgens op **Log in**.