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.

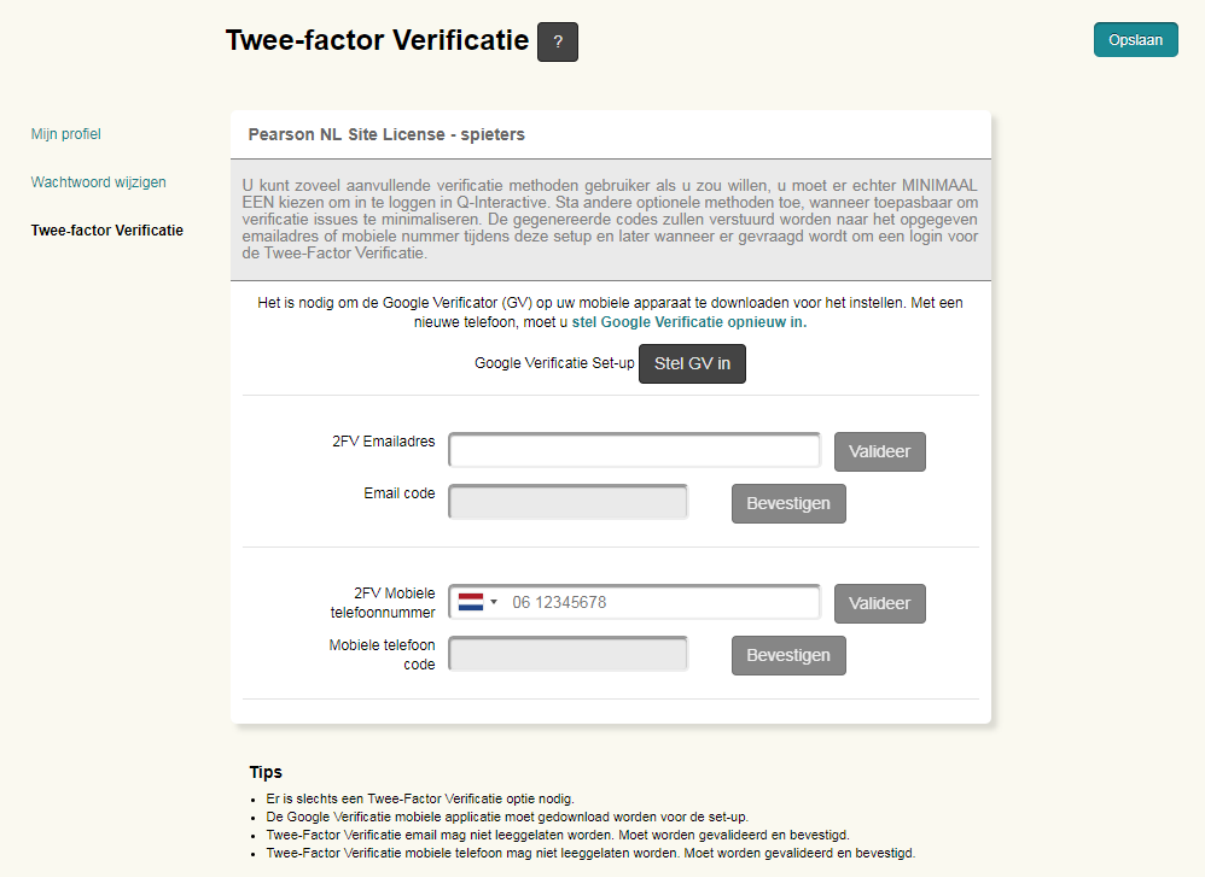
Pearson heeft 2-Factor Authentication ingevoerd op Q-interactive en Q-global om te voldoen aan de vereisten van de nieuwe privacywetgeving GDPR (Algemene Verordening Gegevensbescherming).

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

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.

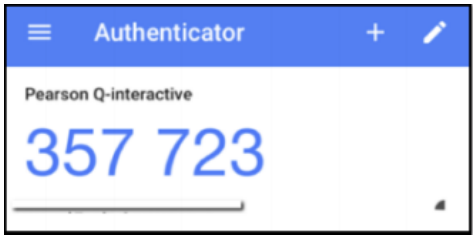


Als u Google Authenticator wilt inschakelen, moet u eerst de app downloaden. Zoek naar "Google Authenticator" in de App Store, Google Play, BlackBerry World of Microsoft Store, afhankelijk van of u een iPhone, Android, BlackBerry of Windows Phone heeft. Zodra Google Authenticator op uw telefoon is geïnstalleerd, 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.

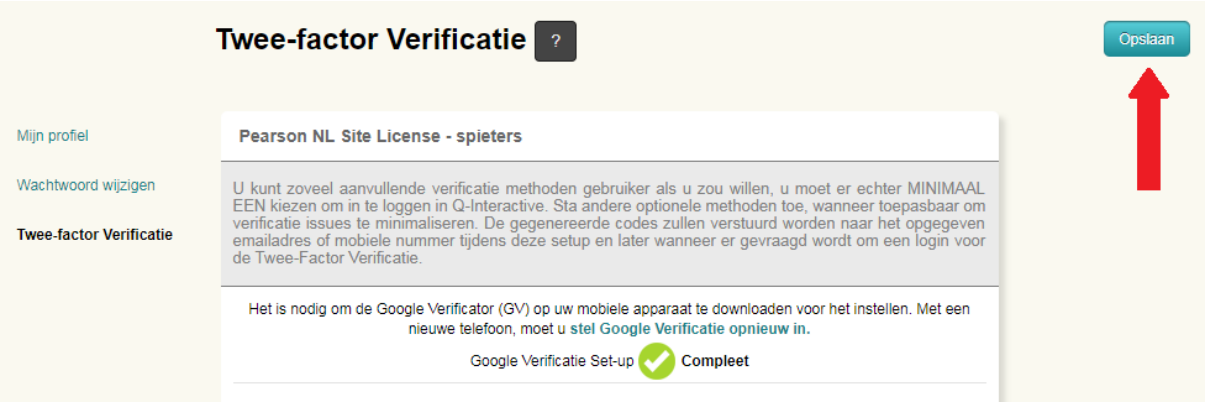
Rechtsboven bevindt zich een QR-code die met de mobiele telefoon kan worden gescand.

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.

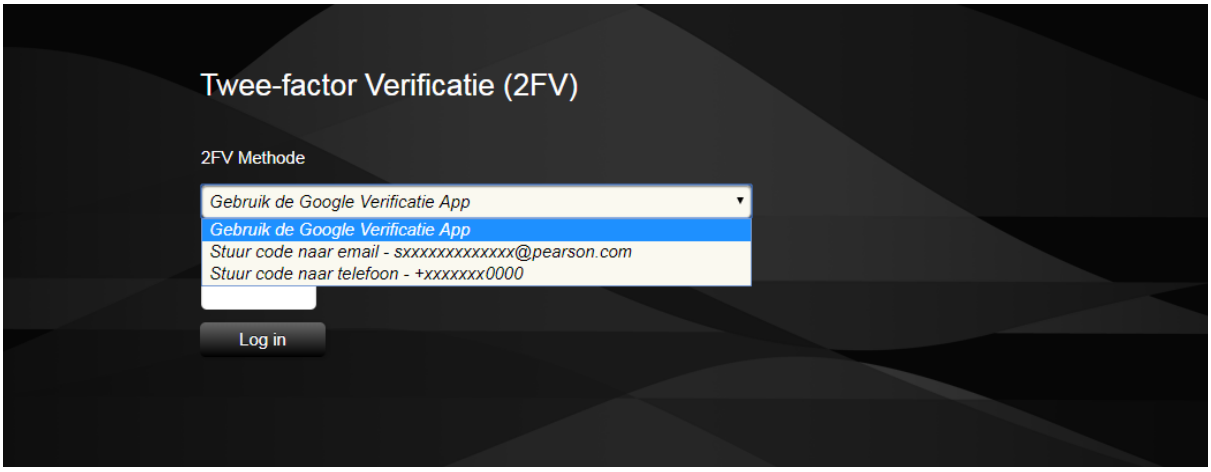


Google Authenticator is nu ingeschakeld in uw account en u moet vanaf nu een zescijferig nummer, gegenereerd door Google Authenticator, invoeren wanneer u zich aanmeldt bij Q-interactive Central en Assess. 2FA is 12 uur geldig op dezelfde computer.

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

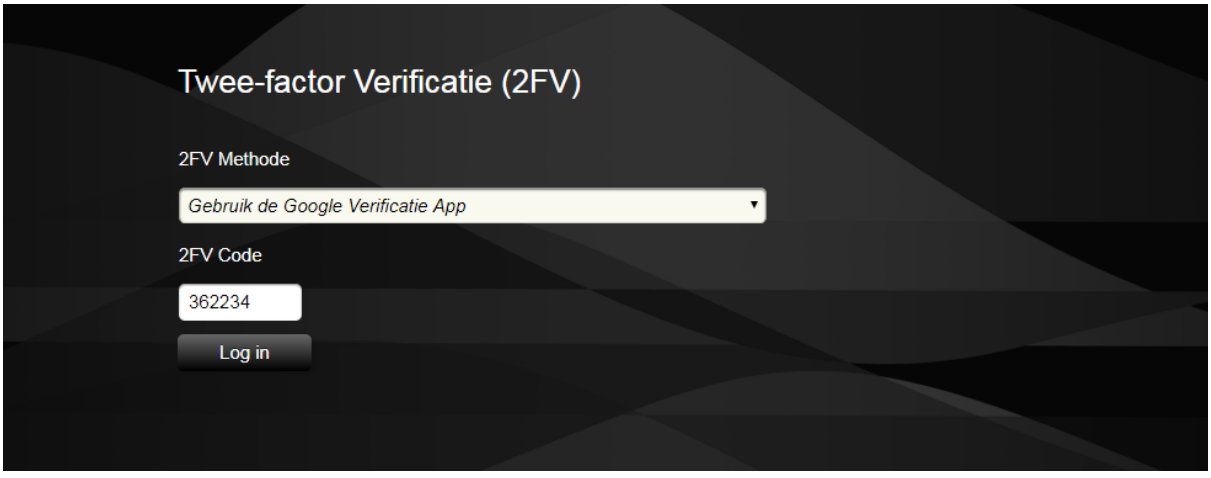
Voer het e-mailadres of mobiele telefoonnummer in en klik op **Valideer**. Er wordt een eenmalige code naar uw e-mailadres of telefoon gestuurd, afhankelijk van de methode die u hebt geselecteerd. Voer de code in het daarvoor bestemde vak in, en klik op **Bevestigen**. Een groene schijf bevestigt dat 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.



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.



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**.