



Q-interactive®

Guide for bruk av tofaktoraутентisering (2FA)

Q-interactive Brukerhåndbok

Februar 2018

Tofaktorautentisering, heretter kalt 2FA, er et supplement til brukernavn og passord, for ytterligere å øke sikkerheten til kontoer på Q-interactive og Q-global. Når man logger inn med 2FA vil man angi brukernavn og passord som vanlig, men også en engangskode som bare du har tilgang til. Slik får man et ekstra sikkerhetsnivå mot at andre får uønsket tilgang til dine data.

Pearson har implementert tofaktorautentisering på Q-interactive og Q-global for å imøtekomme kravene fra den nye personvernforordningen GDPR (General Data Protection Regulation).

Første gang du logger inn før 2FA er aktivert, får du opp et vindu som beskriver hva 2FA er:

Tofaktorautentisering (2FA)

Hva er tofaktoautentisering og hvordan fungerer det?

Tofaktoautentisering er en sikkerhetsfunksjon som hjelper deg å beskytte Q-interactive kontoen din i tillegg til brukernavn og passord. Når tofaktoautentisering er aktivert, blir du bedt om å skrive inn en ekstra sikkerhetskode, eller bekrefte innloggingen din etter at du har skrevet inn ditt brukernavn og passord.

Det er flere autentiseringsmetoder* du kan bruke sammen med din Q-interactive konto for tofaktoautentisering:

- Sikkerhetskoder fra Google Authenticator
- SMS koder fra din registrerte mobiltelefon (avgifter kan tilkomme)
- E-post koder fra din registrerte E-post adresse

Merk: ikke alle autentiseringsmetodene kan være tilgjengelige for deg, avhengig av hva som er aktivert i ditt land.*

Du kan aktivere alle de ekstra autentiseringsmetodene, men du må ha minst én aktivert for å kunne logge inn og bruke Q-interactive.

Må jeg bruke tofaktorautentisering hver gang jeg logger inn?

Du bli bedt om å autentisere med tofaktorautentisering hver 12 time dersom du bruker den samme nettleseren og datamaskinen. Hvis du logger inn med en annen nettleser, eller på en annen datamaskin, vil du bli bedt om å autentisere til og med innenfor det 12 timers intervallet.

Med Assess vil du bli bedt om å autentisere den første gangen du logger inn når du er tilkoblet Internett, på begge dine iPad-er. Du blir gitt valget om å huske din enhet, og dersom du velger dette, må du kun autentisere hver 30 dag. Dersom du velger å ikke huske din enhet, må du autentisere hver 12 time på begge dine enheter.

Vær oppmerksom på at når Assess brukes i Offline-modus blir du ikke bedt om å bruke tofaktorautentisering, og du vil kunne logge inn med ditt vanlige brukernavn og passord.

Du kan aktivere alle de ekstra autentiseringsmetodene, men du må ha minst én aktivert for å kunne logge inn og bruke Q-interactive.

Hvor lenge er kodene på E-post eller SMS gyldig?

Skriv inn 2FA detaljer

Man kan ikke gå videre i applikasjonen før man har konfigurert minst én autentiseringsmetode. Nedenfor presenteres fremgangsmåten for Q-interactive.

Klikk på **Skriv inn 2FA detaljer** for å fortsette.

På neste side kan man angi tre ulike metoder for 2FA: Google Authenticator, SMS eller e-post. Førstnevnte er en kostnadsfri applikasjon som kan lastes ned til de fleste smarttelefoner. Applikasjonen genererer engangskoder som kan brukes for å verifisere innlogging på ulike hjemmesider og programmer. Google Authenticator er enkelt å bruke samt fungerer uten internett og nettverksoppkobling. Applikasjonen genererer nye engangskoder hvert 30. sekund, og er derfor en ganske sikker metode for tofaktorautentisering.

Tofaktorautentisering ? Lagre

Min profil **Pearson QA NO - disaksen_no**

Endre passord

Tofaktorautentisering

Du kan aktivere alle de ekstra autentiseringsmetodene, men du må ha minst én aktivert for å kunne logge inn og bruke Q-interactive. Aktiver andre valgfrie metoder, når det er aktuelt, for å minimere eventuelle autentiseringsproblemer. Genererte koder vil bli sendt til bekreftet E-post eller mobilnummer under denne registreringen, og senere når du blir bedt om å logge inn med tofaktorautentisering.

Det kreves at du laster ned Google Authenticator-appen (GA) til mobilenheten før du konfigurerer den. Med en ny mobil, må du konfigurere Google Authenticator igjen.

Google Authenticator Konfigurering **Konfigurere Google Authenticator**

2FA E-post adresse Validere

E-post kode ✓ Fullført

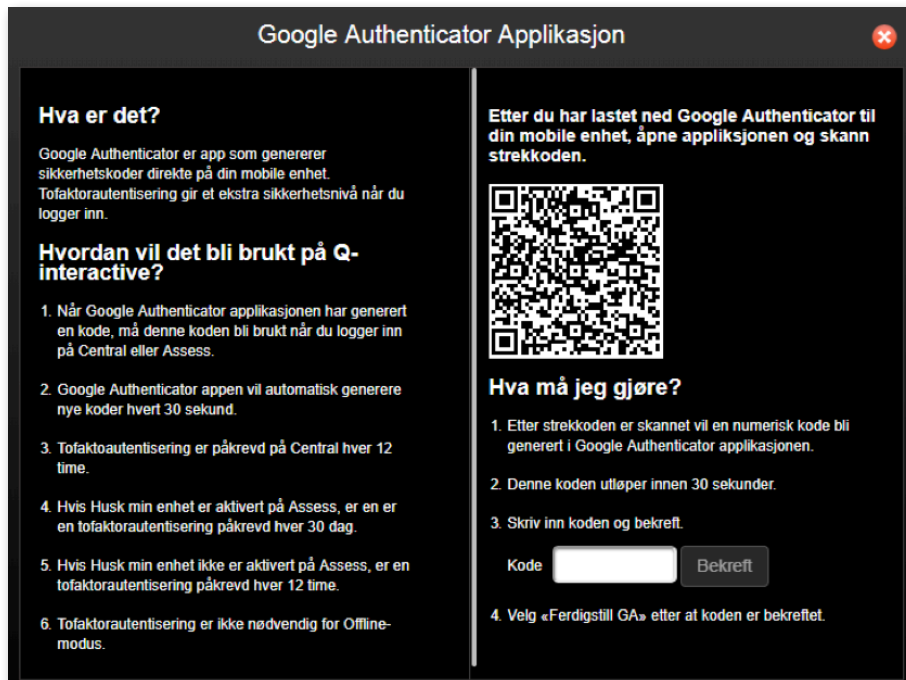
2FA Mobiltelefonnummer Validere

Mobiltelefon kode Bekreft

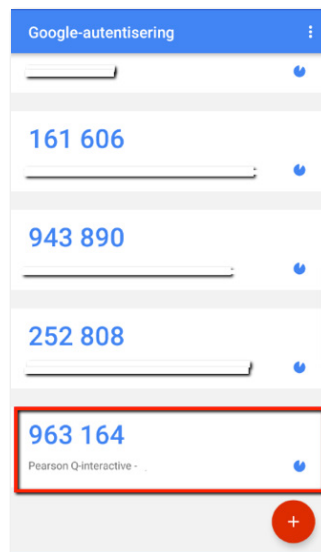
For å *aktivere Google Authenticator*, må du først laste ned applikasjonen. Søk etter "Google Authenticator" i App Store eller Google Play avhengig om du har iPhone- respektive Androidtelefon. Når Google Authenticator er installert på telefonen, går du inn i programmet og trykker på +-tegnet. Velg "Skann en strekkode" og godkjenn eventuelt at applikasjonen får tilgang til kameraet.

Klikk på **Konfigurere Google Authenticator** i Central.

Øverst til høyre finnes en strekkode (QR-kode) som kan skannes med mobiltelefonen.




Ta telefonen og rett kameraet mot strekkoden fra Central slik at strekkoden vises i bildet på telefonen. Et 6-sifret tall presenteres på telefonen:



Angi tallet (6 sifre, mellomrom er ikke nødvendig) i feltet under punkt 3 på Q-interactive Central og klikk på **Bekreft**. En grønn hake vises for å bekrefte at koden er verifisert. Klikk deretter på **Fullfør Google Authenticator**.



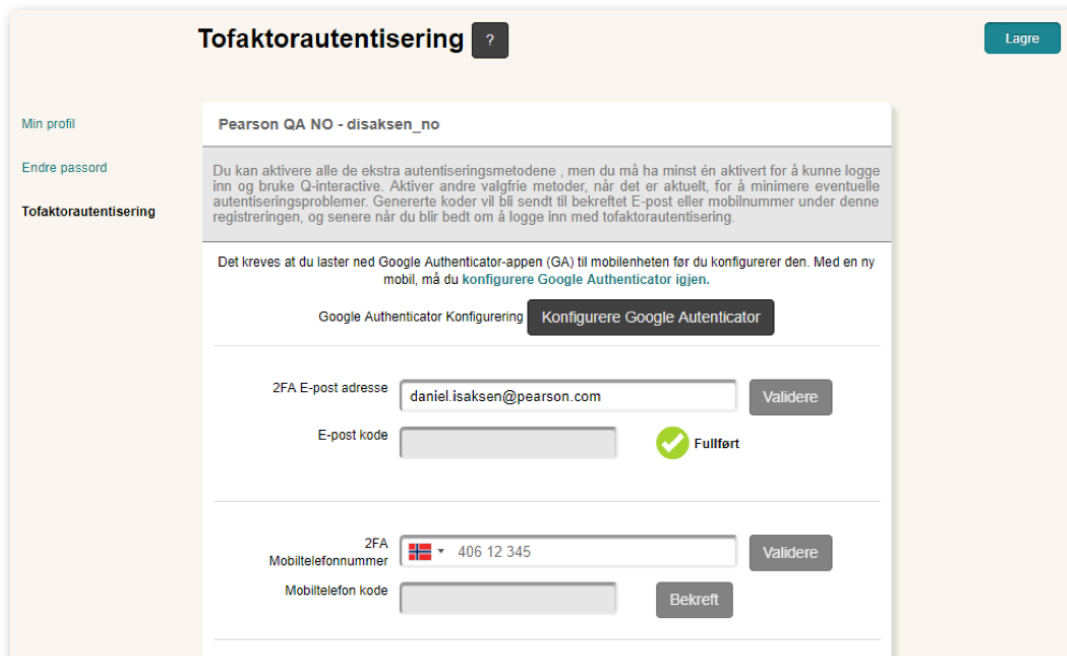
VIKTIG: Kontroller at autentiseringen er fullført. Avslutt ved å klikke på **Lagre** øverst til høyre.



The screenshot shows the 'Tofaktorautentisering' page for user 'Pearson QA NO - disaksen_no'. The 'Tofaktorautentisering' section indicates that Google Authenticator configuration is 'Fullført' (Completed) with a green checkmark. A red arrow points from the 'Fullført' status to the 'Lagre' button in the top right corner.

Google Authenticator er nå aktivert på kontoen og du må angi et 6-sifret tall fra applikasjonen når du logger inn på Central. 2FA-autentiseringen er gyldig i 12 timer på samme datamaskin.

2FA per SMS eller e-post konfigureres på lignende måte.

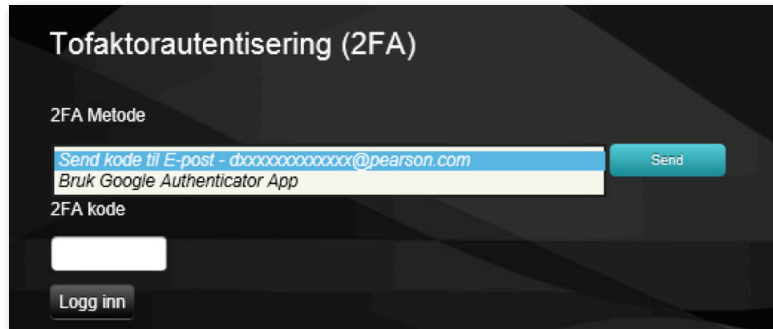


The screenshot shows the 'Tofaktorautentisering' page with the 'Google Authenticator Konfigurering' button disabled. Below it, there are two sections for alternative 2FA methods:

- E-post:** '2FA E-post adresse' is set to 'daniel.isaksen@pearson.com' with a 'Validere' button. Below it, 'E-post kode' is empty, and a green checkmark with 'Fullført' indicates completion.
- Mobiltelefon:** '2FA Mobiltelefonnummer' is set to '406 12 345' with a 'Validere' button. Below it, 'Mobiltelefon kode' is empty, and a 'Bekreft' button is visible.

Angi e-postadresse eller mobiltelefonnummer og klikk på **Validere**. En engangskode sendes til din e-postadresse eller telefon avhengig av den metoden du har valgt. Angi koden i feltet nedenfor og klikk på **Bekreft**. En grønn hake verifiserer at konfigurasjonen er fullført. Husk også her å klikke på **Lagre** øverst til høyre.

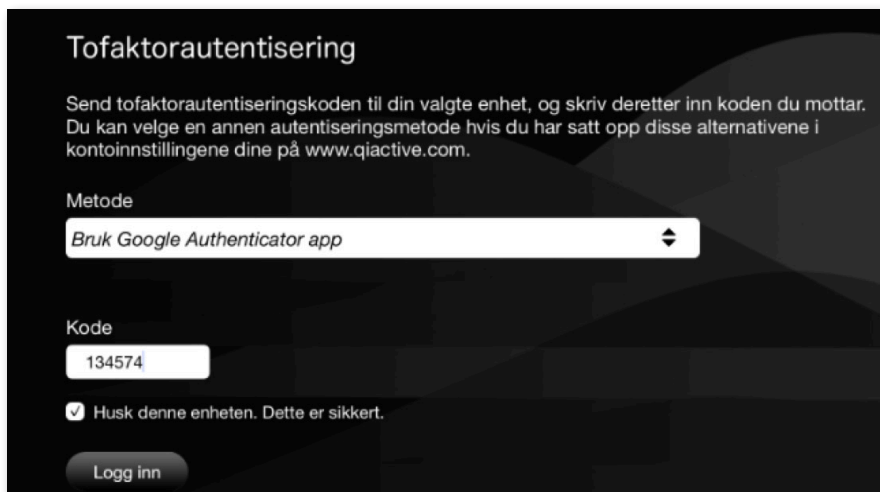
Neste gang du logger inn, får du beskjed om å angi 2FA metode. Dersom du har valgt flere kan du velge mellom en av dem. Velg for eksempel å motta kode per e-post, eller bruk Google Authenticator.



The screenshot shows a dark-themed interface titled "Tofaktorautentisering (2FA)". Under the heading "2FA Metode", there are two radio button options: "Send kode til E-post - dxxxxxxxxxxxx@pearson.com" (which is selected) and "Bruk Google Authenticator App". A blue "Send" button is positioned to the right of the first option. Below this, there is a "2FA kode" label and an empty white input field. At the bottom left, there is a "Logg inn" button.

Angi koden fra Google Authenticator, eller den du får per SMS eller e-post. Klikk på **Logg inn**.

Når man logger inn på Assess på testlederens eller testpersonens iPad, må man også angi engangskoder så lenge iPad-ene er oppkoblet på internett. Angi brukernavn og passord som vanlig. Velg deretter autentiseringsmetode og angi engangskoden på samme måte som når du logger inn på Central.



The screenshot shows a dark-themed interface titled "Tofaktorautentisering". It contains the following text: "Send tofaktorautentiseringskoden til din valgte enhet, og skriv deretter inn koden du mottar. Du kan velge en annen autentiseringsmetode hvis du har satt opp disse alternativene i kontoinnstillingene dine på www.qinteractive.com." Below this is a "Metode" label and a dropdown menu showing "Bruk Google Authenticator app". Underneath is a "Kode" label and a white input field containing the number "134574". There is a checked checkbox with the text "Husk denne enheten. Dette er sikkert." and a "Logg inn" button at the bottom.

Dersom du velger SMS eller e-post, klikk på **Send** og skriv inn koden du mottar.

Klikk deretter på **Logg inn**.