Q-interactive®

Guide for bruk av tofaktorautentisering (2FA)

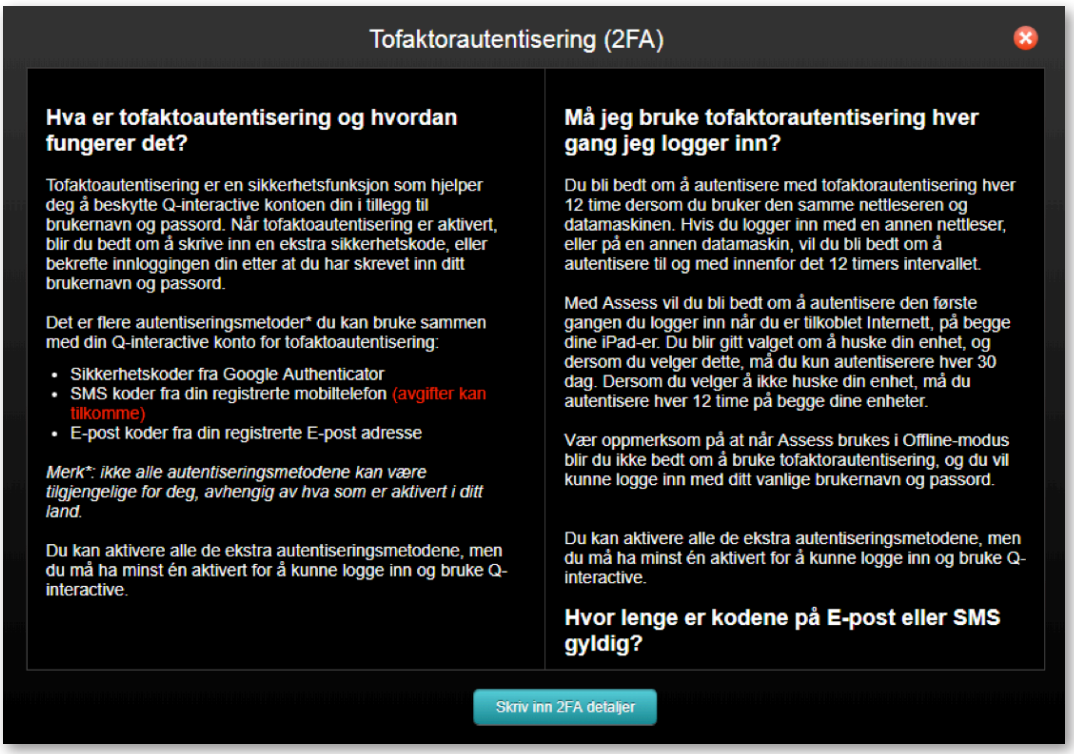
Q-interactive Brukerhåndbok

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).

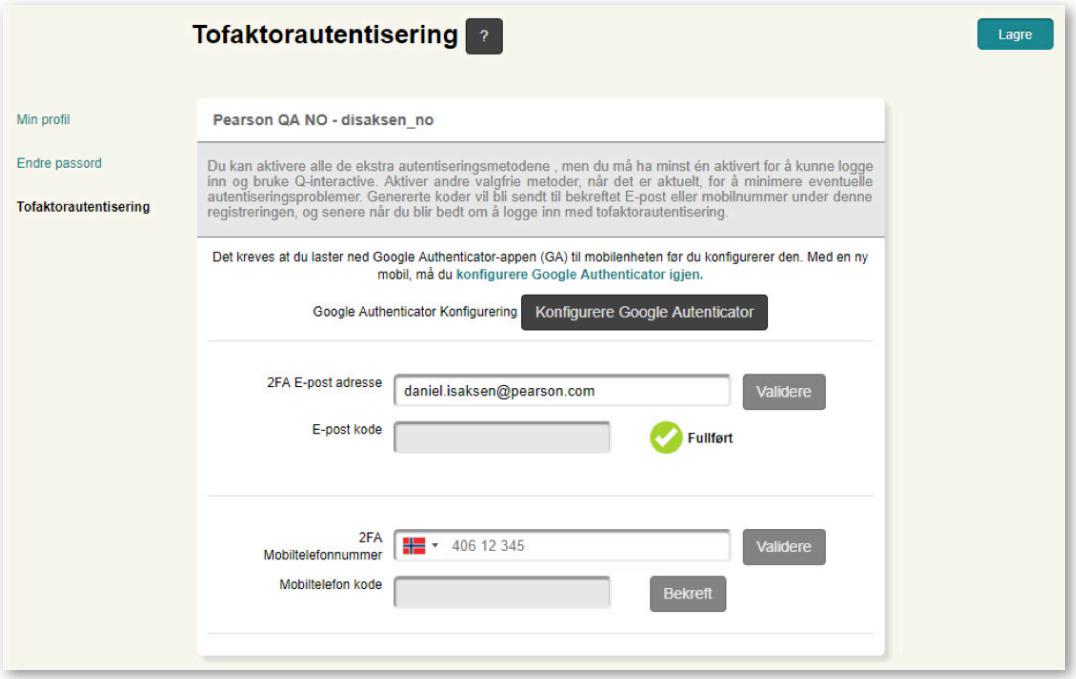
Første gang du logger inn før 2FA er aktivert, får du opp et vindu som beskriver hva 2FA er:



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.

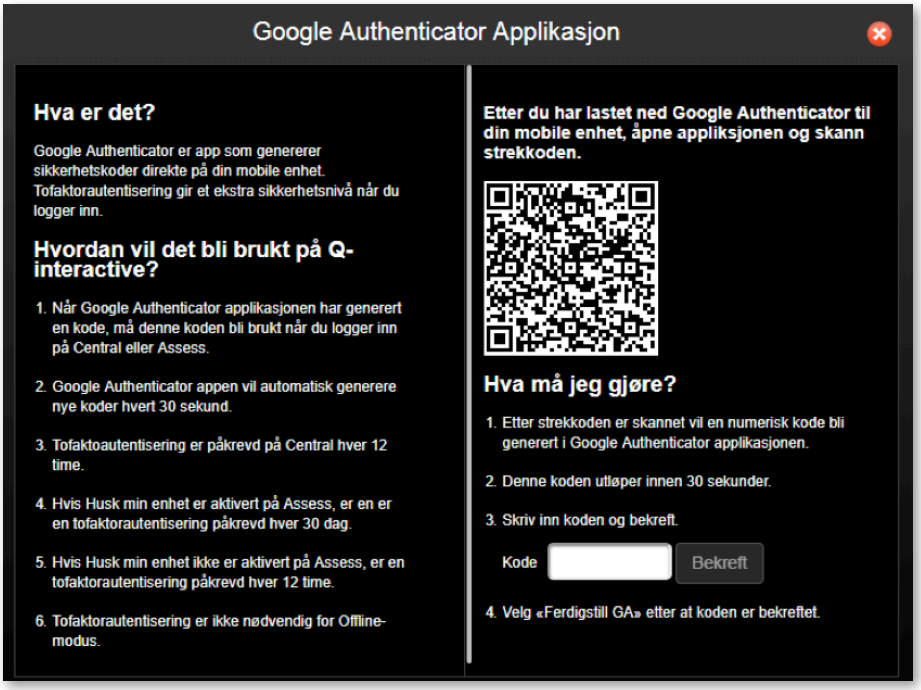
På neste side kan man angi tre ulike metoder for 2FA: Google Authenticator, SMS eller e-post. Førstnevnte er en kostnadsfri applikasjon som kan lastes ned til de fleste smarttelefoner. Applikasjonen genererer engangskoder som kan brukes for å verifisere innlogging på ulike hjemmesider og programmer. 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.



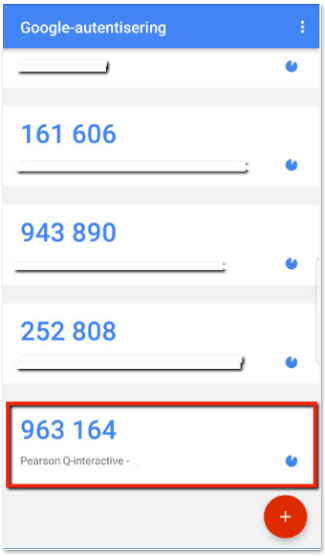
For å *aktivere Google Authenticator*, må du først laste ned applikasjonen. Søk etter ”Google Authenticator” i App Store eller Google Play avhengig om du har iPhone- respektive Androidtelefon. Når Google Authenticator er installert på telefonen, går du inn i programmet og trykker på +-tegnet. Velg ”Skann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

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

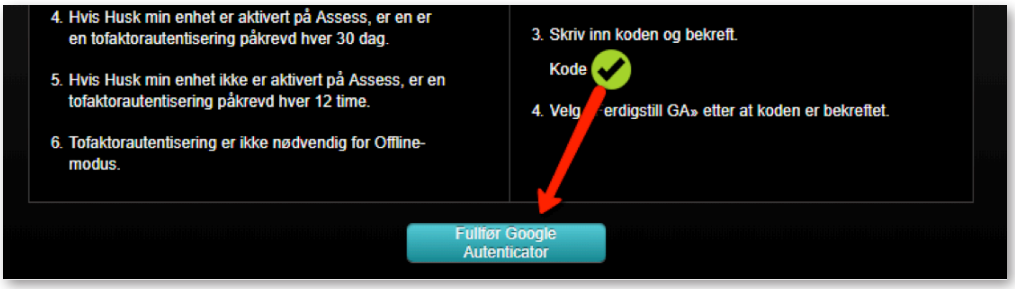
Øverst til høyre finnes en strekkode (QR-kode) som kan skannes med mobiltelefonen.



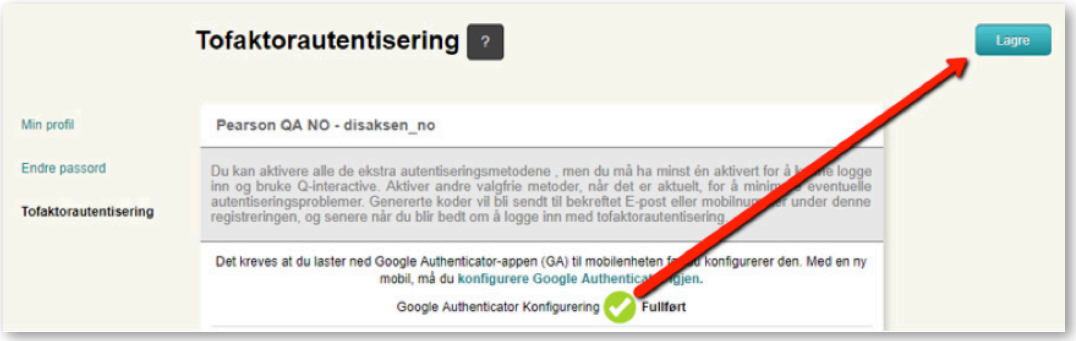
Ta telefonen og rett kameraet mot strekkoden fra Central slik at strekkoden vises i bildet på telefonen. Et 6-sifret tall presenteres på telefonen:



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**.

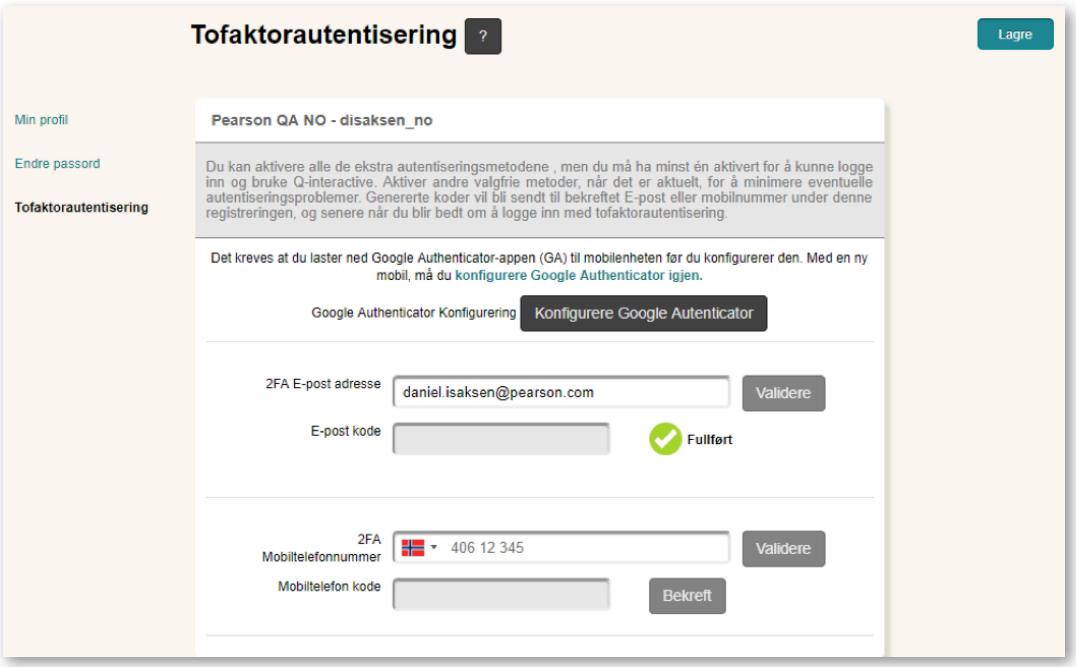


VIKTIG: Kontroller at autentiseringen er fullført. Avslutt ved å klikke på **Lagre** øverst til høyre.



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.

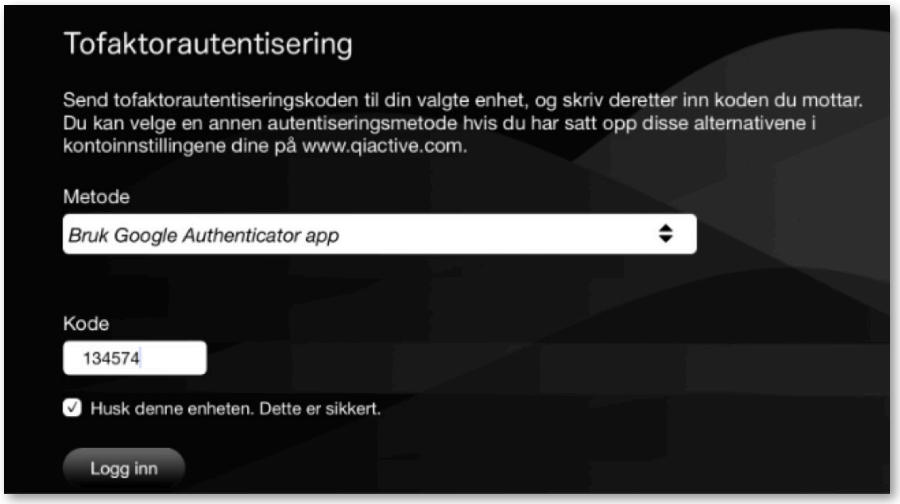


Angi e-postadresse eller mobiltelefonnummer og klikk på **Validere**. En engangskode sendes til din e-postadresse eller telefon avhengig av den metoden du har valgt. Angi koden i feltet nedenfor og klikk på **Bekreft**. En grønn hake verifiserer at konfigurasjonen er fullført. Husk også her å klikke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

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.



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

Klikk deretter på **Logg inn**.